

# PROJETO BÁSICO COGTI 832/2012

## Título

### Consulta Pública para Aquisição de Soluções de Firewall

#### 1.0 Objeto

Consulta Pública para aquisição de soluções de Firewall, com criação de Ata de Registro de Preços.

#### 2.0 Especificação do Objeto

Consulta Pública para aprimorar aos itens para aquisição de várias de soluções de Firewalls para ambientes de serviços do Serpro com as seguintes especificações:

##### 2.1. ITEM I – FIREWALL PROJETO RECEITA FEDERAL DO BRASIL

Solução integrada de Cluster de Firewall e Gerência, baseados em hardware, software e suporte técnico. Essa Solução que deverá ser fornecida com 02 (dois) clusters de firewall, sendo 01 (um) cluster para a localidade de São Paulo e 01 (um) cluster para a localidade de Brasília, configurados em cluster de alta-disponibilidade, com no mínimo 02 appliances físicos cada cluster e com as seguintes características de hardware e software entre si:

##### 2.1.1. Características de hardware por equipamento (appliance)

2.1.1.1. Throughput mínimo de 20 (vinte) Gbps para firewall, usando-se como base o padrão IMIX (57% de pacotes de 64bytes, 23% de pacotes de 570bytes e 20% de pacotes de 1518bytes) (AMOSTRA);

2.1.1.2. Throughput mínimo de 04 (quatro) Gbps para VPN IPSec, com criptografia 3DES/AES;

2.1.1.3. Possibilitar 3.000.000 (três milhões) de conexões simultâneas ;

2.1.1.4. Possibilitar 4.500.00 (quatro milhões e quinhentos mil) pacotes por segundo (PPS) (AMOSTRA);

2.1.1.5. Possibilitar 300.000 (trezentas mil) conexões por segundo (AMOSTRA);

2.1.1.6. Prover configuração de memória (RAM, Flash) contemplando a capacidade máxima para o modelo ofertado;

2.1.1.7. As seguintes interfaces deverão estar livres para produção em cada equipamento de firewall:

2.1.1.7.1. No mínimo, 6 (seis) interfaces de 10 Gigabit Ethernet padrão SFP+ e 8 (oito) interfaces Gigabit Ethernet 1000Mbps para cabeamento de cobre, com possibilidade de expansão por módulos. As interfaces de rede devem ser todas frontais;

2.1.1.8. Deve suportar a definição de VLAN no firewall conforme padrão IEEE 802.1q e ser possível criar pelo menos 1024 (mil e vinte e quatro) interfaces ou subinterfaces lógicas associadas a VLANs e estabelecer regras de filtragem (Stateful Firewall) entre elas.

2.1.1.9. Possuir uma interface serial, para configuração e gerenciamento através de interface de linha de comando (CLI);

2.1.1.10. Possuir 02 (duas) fontes de alimentação independentes e redundantes, com tensão de entrada de 120V a 240V AC (manual ou automática), e frequência de 60Hz (AMOSTRA);

2.1.1.11. Possuir led indicativo de on/off;

2.1.1.12. A utilização de equipamentos modulares (compostos por mais de um appliance) é permitida, desde que atendidas as funcionalidades exigidas para cada equipamento de firewall;

2.1.1.13. Os equipamentos deverão ser instalados em um rack fornecido juntamente com os mesmos, padrão EIA-310, com largura de 19 polegadas, altura de 42U, e ventilação forçada, devendo ser incluído o fornecimento de todos os cabos e suportes (se necessários, "gavetas", "braços" e "trilhos") para a instalação dos equipamentos no rack;

## **2.1.2. Características do software de firewall e VPN**

2.1.2.1. Sem restrições de número máximo de máquinas protegidas;

2.1.2.2. Possuir sistema operacional customizado especificamente para funções de firewall.

Não serão aceitos sistemas de firewall que sejam executados sobre sistemas operacionais de mercado;

2.1.2.3. Prover mecanismo de conversão de endereços NAT (Network Address Translation), de forma a possibilitar que: (AMOSTRA):

2.1.2.3.1. Realizar NAT estático (1-1), dinâmico (N-1), NAT pool (N-N) e NAT condicional, possibilitando que um endereço tenha mais de um NAT dependendo da origem, destino ou porta; (Amostra) (AMOSTRA))

2.1.2.3.2. Redes ou faixas de endereços IP reservados acessem a Internet a partir de um ou mais endereços IP públicos (Dynamic NAT); (AMOSTRA)

2.1.2.3.3. Permitir o registro de eventos de NAT contendo as informações de endereço interno, endereço público, data e hora do evento, portas de origem e destino;

2.1.2.3.4. Nat condicional em relação aos segmentos de origem/destino, possibilitando que um endereço interno tenha mais de um endereço de nat, dependendo da rede destino;

2.1.2.4. Fornecer criptografia e autenticação de pacotes IP, com chaves de criptografia de, 3DES/AES, no mínimo, de forma a possibilitar a criação de canais seguros ou IPSEC VPNs;

2.1.2.5. Compatibilidade com o padrão IPSEC, de acordo com as RFCs 2401 a 2412, de modo a estabelecer canais de criptografia com outros produtos que também suportem tal padrão;

2.1.2.6. Permitir a criação de VPN site-to-site e client-to-site;

2.1.2.7. Possibilitar o controle do tráfego para os protocolos TCP, UDP e ICMP baseados nos endereços de origem e destino e no serviço utilizado em uma comunicação;

2.1.2.8. Possibilitar o controle do tráfego para os protocolos GRE, H323, e IGMP baseados nos endereços origem e destino da comunicação;

2.1.2.9. Implementar QoS conforme arquitetura “Differentiated Services” (DiffServ) (RFCs 2474 e 2475);

2.1.2.10. Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, Real Áudio, Real Vídeo e RTSP, SIP, H323, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para tráfego outbound (de dentro para fora) quanto inbound (de fora para dentro);

2.1.2.11. A solução de Firewall deve funcionar em cluster do tipo ativo-standby ou ativo-ativo com o balanceamento interno(AMOSTRA);

2.1.2.11.1. Os firewalls deverão ser configurados em “paralelo”, e no caso de falha em um dos nós, o(s) remanescente(s) deverá(ão) assumir o controle automaticamente;

2.1.2.11.2. Na ocorrência de falhas, as conexões existentes em um firewall deverão ser mantidas pelo(s) outro(s) sem perdas destas conexões, não acarretando interrupções no tráfego da rede e nem redução de desempenho da solução;

2.1.2.11.3. Na instalação de regras as conexões existentes deverão ser mantidas sem perda das conexões ativas;

2.1.2.12. Na configuração de alta-disponibilidade todas as configurações e estados de conexões devem ser replicados entre os firewalls do cluster;

2.1.2.13. No caso de falha de um dos nós, as conexões ativas (IPSEC-VPN inclusive) devem continuar funcionando através do(s) outro(s) firewall(s) do cluster. Não poderão haver perdas de conexões ativas através do cluster mesmo que estas passem por NAT ou VPN;

2.1.2.14. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma comunicação deve se originar;

2.1.2.15 Suportar anti-spoofing (sem uso de ACLs) para endereços IPv4 e IPv6;

2.1.2.16. Prover mecanismo contra ataques de negação de serviço (DoS) e SYN Flood, repassando somente as conexões estabelecidas entre os segmentos;

2.1.2.17. Promover a integração com diretórios LDAP (X.500) e Active Directory para a autenticação de usuários, de modo que o Firewall possa utilizar das informações armazenadas para realizar autenticações;

- 2.1.2.18. Suportar os seguintes esquemas de autenticação de usuários por VPN: usuário e senha em base do próprio sistema de Firewall, diretório LDAP, certificação digital por meio de certificados emitidos por Autoridade Certificadora no padrão ICP-Brasil com suporte para SHA-1 e SHA-2;
- 2.1.2.19 Suportar o protocolo DHCP no modo relay;
- 2.1.2.20. Suportar SNMP v3, H.323 v2, 3 e 4, H.225 v2, 3 e 4, H.245, NAT para H.323;
- 2.1.2.21. Integração com MIBs que possam ser compiladas para o sistema de gerenciamento SNMP;
- 2.1.2.22. Suportar a configuração de agregação de interfaces, conforme padrão IEEE 802.1q;
- 2.1.2.23. Suportar inspeção stateful de tráfego IPv4 e Ipv6;
- 2.1.2.24. Suportar simultaneamente a criação de regras IPv4 e Ipv6;
- 2.1.2.25. Suportar roteamento estático de tráfego Ipv6;
- 2.1.2.26. Suportar gerenciamento sobre IPv4 e IPv6 com criptografia;
- 2.1.2.27. Suportar stateful failover de conexões IPv6, sem que haja prejuízo do funcionamento das demais especificações;
- 2.1.2.28. Possibilitar implementação de firewall tanto em modo transparente como também em modo gateway (roteado);
- 2.1.2.29. Suportar agrupamento lógico de objetos IPv6 (redes, hosts, serviços) e criação de regras (ACLs) usando tais objetos ;
- 2.1.2.30. Possuir uma ferramenta de captura de pacotes (AMOSTRA);
- 2.1.2.31. O sistema operacional deverá ser customizado pelo próprio fabricante do firewall para garantir segurança e melhor performance ao firewall, permitindo o monitoramento de recursos no appliance;
- 2.1.2.32. Deve permitir a criação de rotas estáticas e suportar OSPF ou BGP;
- 2.1.2.33. Suportar a definição de VLAN trunking no firewall conforme padrão IEEE 802.1q;
- 2.1.2.34. Possibilitar a criação de pelo menos 1024 (mil e vinte e quatro) interfaces ou subinterfaces lógicas associadas a VLANs e estabelecer regras de filtragem (Stateful Firewall) entre elas. Deve ser possível a utilização de TAG até 4096 (AMOSTRA);
- 2.1.2.35. Possibilitar que as regras de filtragem tenham a capacidade de implementação de CIDR/VLSM;
- 2.1.2.36. Possibilitar a atuação como cliente NTP (Network Time Protocol), conforme RFC 1305, contemplando autenticação MD5 entre os peers;
- 2.1.2.37. Possibilitar a construção de registro de fluxos de dados relativos a cada sessão iniciada armazenando para cada uma destas sessões informações tais como: endereços (IPv4 e IPv6) de origem e destino dos pacotes, traduções NAT, portas TCP e UDP de origem e destino, bem como números de seqüência dos pacotes TCP e UDP, status dos flags “ACK”, “SYN” e “FIN”, facilitando assim o controle de todo tráfego que passa ou é negado pelo Firewall e aplicação da política de segurança (AMOSTRA);
- 2.1.2.38. Possibilitar a aplicação de novas regras sem provocar indisponibilidade de serviço, isto é, permitindo que conexões ativas ou pendentes não sofram descontinuidade no sistema de firewall (AMOSTRA);

### **2.1.3. Características comuns de administração, gerenciamento, e auditoria quanto a configuração, administração, e gerenciamento dos firewalls e seus clusters**

- 2.1.3.1. Disponibilizar, através de interface serial ou das interfaces de rede, a configuração e gerenciamento dos firewalls por linha de comando CLI (emulação de terminal Telnet ou SSH), ou via Web (HTTP ou HTTPS);
- 2.1.3.2. Possuir criptografia na comunicação através de protocolo seguro;
- 2.1.3.3. Prover mecanismos de restrição de acesso remoto, através de filtros de endereços IP e usuário/senha;
- 2.1.3.4. Prover meios para criar, modificar, e excluir (além do padrão de fábrica) novos usuários e grupos administradores, pelo menos 02 (dois), com diferentes níveis de acesso (ex.: acesso total, leitura e escrita, somente leitura e outros níveis);
- 2.1.3.5. Permitir a conexão simultânea de vários usuários administradores. O acesso simultâneo destes não deverá comprometer a base de dados;

- 2.1.3.6. Prover meios para criar, modificar, e excluir regras de acesso, através de, no mínimo:
  - 2.1.3.6.1. Endereços IP de host(s);
  - 2.1.3.6.2. Endereços IP de rede(s);
  - 2.1.3.6.3. Protocolos e portas (TCP, UDP e ICMP);
  - 2.1.3.6.4. Dias, mês, ano e horários determinados.
- 2.1.3.7. Permitir que a administração remota de cada firewall possa ser feita através de um módulo de gerenciamento centralizado (item 2.1.2);
- 2.1.3.8. Possuir criptografia forte na comunicação com o equipamento de gerenciamento;
- 2.1.3.9. Possuir sistema que possibilite alertar imediatamente o administrador através de e-mails, janelas gráficas de alerta, e envio de traps SNMP;
- 2.1.3.10. Permitir a visualização em realtime (tempo-real) de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall;
- 2.1.3.11. Permitir a visualização de estatísticas do uso de CPU, memória ou utilização do hardware onde o firewall está funcionando;
- 2.1.3.12. Possibilitar o registro de toda ocorrência de mudanças nas configurações e demais aspectos importantes para auditoria do sistema;
- 2.1.3.13. Permitir o registro de toda a comunicação realizada através do firewall, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo;
- 2.1.3.14. Permitir o armazenamento e recuperação, através de protocolo criptografado, dos logs e eventos em máquinas remotas e servidores de consolidação de logs, Syslog, ou Syslog-ng;
- 2.1.3.15. Possibilitar, a partir da console gráfica de gerenciamento (item 2.2) e através de protocolo criptografado, a recuperação dos registros de log e eventos armazenados;
- 2.1.3.16. Possibilitar a aplicação de correções e atualizações para o sistema operacional e de firewall;
- 2.1.3.17. Oferecer ajuda on-line em inglês ou português;
- 2.1.3.18. A solução deve estar em linha de fabricação na data de abertura do certame licitatório, bem como deve ser garantida a continuidade no suporte nos próximos 5 (cinco) anos;
- 2.1.3.19. A contratada será responsável pela migração integral das políticas, regras, NATs, rotas, objetos e demais parâmetros que se façam necessários para a reprodução completa do cenário operacional para a nova solução, que configura a implantação total da solução. O volume de objetos de rede a serem migrados é da ordem de, aproximadamente, 8000 (oito mil) objetos de rede, considerando as duas localidades (São Paulo e Brasília).

#### **2.1.4. Solução de Gerencia Centralizado de firewalls**

Deverão ser fornecidas 2 (duas) soluções de Gerência, com alta disponibilidade (uma solução para cada cluster de firewall's (item 2.1) em servidores distintos) , sendo 01 (uma) solução de Gerência com alta disponibilidade para São Paulo e 01 (uma) solução de Gerência com alta disponibilidade para Brasília, independentes entre si, com licenças de sistema operacional necessárias para seu correto funcionamento.

##### **2.1.4.1. Características mínimas exigidas do hardware**

- 2.1.4.1.1. Fornecer equipamentos com capacidade de suportar o gerenciamento de no mínimo 2(dois) clusters de firewall simultaneamente com acesso privilegiado, com capacidade de armazenamento mensal de logs de todas as paredes, estimando no mínimo 5 Terabytes mensais;
- 2.1.4.1.2. Possuir no mínimo 02 (duas) interfaces de rede Gigabit Ethernet 1000Mbps (compatíveis com o padrão IEEE 802.3), com conectores RJ45 (AMOSTRA);
- 2.1.4.1.3. Possuir 02 (duas) fontes de alimentação independentes e redundantes, com tensão de entrada de 120V a 240V AC (manual ou automática), e frequência de 60Hz (AMOSTRA);

##### **2.1.4.2. Características do software de gerenciamento e administração**

- 2.1.4.2.1. Disponibilizar, através de interface serial ou das interfaces de rede, a configuração e gerenciamento dos firewalls por linha de comando CLI (emulação de terminal Telnet ou SSH),

ou via Web (HTTP ou HTTPS);

2.1.4.2.2. Possuir criptografia na comunicação através de protocolo seguro;

2.1.4.2.3. Possibilitar conexão remota de vários usuários simultâneos;

2.1.4.2.4. Fornecer mecanismos de restrição de acesso remoto, através de filtros de endereços IP, e usuário/senha;

2.1.4.2.5. Toda a comunicação entre a solução de gerenciamento centralizado e os firewalls deve ser segura;

2.1.4.2.6. Permitir a instalação na configuração de alta-disponibilidade por tolerância a falhas, onde:

2.1.4.2.6.1. Deverão ser configurados em “paralelo”, e no caso de falha de um dos módulos de Gerenciamento Centralizado, o(s) remanescente(s) deverá(ão) assumir automaticamente todas as funcionalidades de administração dos firewalls e seus clusters gerenciados;

2.1.4.2.6.2. Permitir o retorno das funcionalidades do Módulo de Gerenciamento primário após a recuperação do mesmo;

2.1.4.2.6.3. Deverá haver uma replicação (incremental ou diferencial) das bases de dados de objetos, políticas, regras e configurações entre os módulos;

2.1.4.2.6.4. Permitir que os registros de logs e eventos dos firewalls administrados sejam armazenados em tempo real, nos servidores de gerenciamento, para que no caso de falha no sistema de gerência primaria o(s) remanescente(s) assumam(m) com as mesmas características e funcionalidades;

2.1.4.2.7. Deve permitir acesso à console de gerência através de Web, cliente compatível com sistemas operacionais Microsoft Windows e GNU Linux ou cliente compatível com protocolo RDP (Remote Desktop Protocol); (AMOSTRA)

2.1.4.2.8. Fornecer segurança criptográfica para acesso a console gráfica de gerenciamento remoto;

#### **2.1.4.2.9. A console gráfica deve fornecer, pelo menos, as seguintes opções de gerenciamento**

2.1.4.2.9.1. Gerenciamento remoto de múltiplos firewalls simultaneamente, sem a necessidade de se executar várias consoles gráficas;

2.1.4.2.9.2. Permitir que os firewalls sejam colocados em grupos distintos e que passem a herdar somente as configurações associadas a tais grupos;

2.1.4.2.9.3. Permitir a criação de regras centralizadas, de forma que possam ser aplicadas a diversos grupos de firewalls de maneira automática;

2.1.4.2.9.4. Prover meios para criar, modificar, e excluir novos usuários e grupos administradores, com diferentes níveis de acesso;

2.1.4.2.9.5. Permitir a conexão simultânea de vários usuários administradores. O acesso simultâneo destes não deverá comprometer a base de dados;

2.1.4.2.9.6. Possibilitar o gerenciamento (incluindo a criação, alteração, monitoração e exclusão) de objetos de rede. Deverá ainda permitir detectar se e onde, na base de regras, está sendo utilizado determinado objeto de rede. Os tipos de objetos deverão permitir especificar de forma distinta recurso tais como (AMOSTRA):

2.1.4.2.9.6.1. Hosts;

2.1.4.2.9.6.2. Gateways;

2.1.4.2.9.6.3. Firewalls;

2.1.4.2.9.6.4. Clusters (alta-disponibilidade);

2.1.4.2.9.6.5. Redes;

2.1.4.2.9.6.6. Faixas de endereços;

2.1.4.2.9.6.7. NAT;

2.1.4.2.9.6.8. Usuários;

2.1.4.2.9.6.9. Agrupamento de objetos;

2.1.4.2.9.6.10. VPNs (Client-to site e Site-to-site);

2.1.4.2.10. Os objetos de rede deverão ser dos tipos Globais, objetos disponíveis para uso em todos os equipamentos de firewall administrados, e Locais, objetos disponíveis para uso apenas em um firewall ou grupos de firewall para os quais foram criados;

- 2.1.4.2.11. Possibilitar o gerenciamento (incluindo a criação, alteração, monitoração e exclusão) de regras de acesso no módulo de firewall descrito anteriormente (item 2.1), de forma individual para cada firewall, ou generalizada, em todos os módulos de firewall administrados;
- 2.1.4.2.12. As regras descritas no item anterior devem, no mínimo, definir ações como: Accept (aceitar); Drop (interromper); Encrypt (encriptar);
- 2.1.4.2.13. Suportar agrupamento lógico de objetos (“object grouping”) para criação de regras de filtragem;
- 2.1.4.2.14. Permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras em todos os clusters;
- 2.1.4.2.15. Possibilitar a especificação de política por tempo, ou seja, permitir a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora) (AMOSTRA);
- 2.1.4.2.16. O licenciamento e o software não devem limitar o número de objetos, regras de segurança, NAT, endereços IP e usuários de VPN SSL;
- 2.1.4.2.17. Possibilitar configurar, de forma gráfica, a solução de Firewall provida pelo fabricante da solução;
- 2.1.4.2.18. Suportar usuários com acesso somente-leitura;
- 2.1.4.2.19. Possuir ferramenta de análise de consistência das regras para evitar conflitos lógicos entre novas regras e regras existentes;
- 2.1.4.2.20. Implementar a contabilização das Regras de Controle de Acesso por ela gerenciados;
- 2.1.4.2.21. Permitir o agrupamento lógico de dispositivos físicos permitindo o gerenciamento simultâneo de vários elementos;
- 2.1.4.2.22. Permitir a reutilização de objetos lógicos em várias políticas de Segurança (AMOSTRA);
- 2.1.4.2.23. Permitir o retorno emergencial às configurações anteriores dos dispositivos, para a necessidade de recuperação de falhas (“Rollback de configuração”);
- 2.1.4.2.24. Permitir distribuição centralizada de pacotes de atualização;
- 2.1.4.2.25. Permitir testar a conectividade dos equipamentos gerenciados;
- 2.1.4.2.26. Suportar configuração das funcionalidades de alta disponibilidade dos dispositivos físicos;
- 2.1.4.2.27. Permitir a visualização de qual parte da topologia gerenciada (origem, destino, serviço) está sendo afetada por determinada regra;
- 2.1.4.2.28. Permitir a detecção de alteração e tentativas de alteração da configuração dos dispositivos físicos e avisar o administrador (acessos que não usem a interface de gráfica de gerência provida pela ferramenta);
- 2.1.4.2.29. Implementar funcionalidade de agrupamento de políticas de Segurança, ou seja, detectar um conjunto de regras que possa ser condensado em uma única regra que venha a produzir o mesmo efeito lógico no que concerne a Políticas de Segurança;
- 2.1.4.2.30. Suportar operação em modo de “workflow”, ou seja, permitir que as regras sejam aplicadas somente após passar por um fluxo de aprovação gerencial;
- 2.1.4.2.31. Suportar acesso baseado em perfil de usuário com as permissões de visualizar, modificar, aprovar e distribuir por tipo de objeto e política;
- 2.1.4.2.32. Possibilitar definir os perfis de acesso à solução (“Role Based Access Control” = RBAC) no sistema de Gerência de Controle de Acesso fornecido;
- 2.1.4.2.33. Permitir a identificação e exclusão de regras que estão aplicadas nos dispositivos, mas não afetam o desempenho e a segurança da rede (regras em desuso sob o ponto de vista lógico);
- 2.1.4.2.34. Suportar protocolo de autenticação para controle do acesso administrativo ao equipamento que possua pelo menos as seguintes características:
- 2.1.4.2.34.1. Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega;
- 2.1.4.2.34.2. Cifrar todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;

- 2.1.4.2.34.3. Registrar todos os comandos executados por um dado usuário(accounting);
- 2.1.4.2.34.4. Permitir atribuição de perfis incluindo: usuário (somente leitura), administradores e monitores com níveis de permissão diferenciados.
- 2.1.4.2.35. Fornecer as informações detalhadas em realtime (tempo-real), ou com o menor atraso possível, além de relatórios e logs detalhados contendo, no mínimo: data e horário de acesso; recursos acessados por máquina; estatísticas de uso, conexões, VPNs IPSEC estabelecidas, processamento, memória, configurações e estados de cada um dos equipamentos de firewall (item 2.1), informações de estado de clusters de alta-disponibilidade;
- 2.1.4.2.36. Implementar coleta de informações estatísticas sobre o tráfego passando através do módulo de firewall, possibilitando a geração automática de relatórios e gráficos que discriminem o tráfego por regra de filtragem e por endereço IP;
- 2.1.4.2.37. Possibilitar a monitoração de toda a comunicação realizada ou bloqueada através do módulo de firewall gerenciado, além de todas as ocorrências de mudanças nas suas configurações e demais aspectos importantes para auditoria do módulo de firewall;
- 2.1.4.2.38. Permitir o armazenamento, através de protocolo criptografado, dos logs e eventos dos firewalls gerenciados, em máquinas remotas e servidores de consolidação de logs, Syslog ou Syslog-ng;
- 2.1.4.2.39. Possibilitar, através de protocolo criptografado, a recuperação dos registros de log e eventos armazenados nos servidores listados no item anterior;
- 2.1.4.2.40. Permitir a geração de relatórios e gráficos a partir dos registros de eventos e logs dos firewalls gerenciados;
- 2.1.4.2.41. Possibilitar a aplicação remota de correções e atualizações para os módulos de firewall descritos anteriormente;
- 2.1.4.2.42. Possibilitar a aplicação de correções e atualizações para o sistema operacional e a console gráfica de gerenciamento;
- 2.1.4.2.43. Possuir suporte ao protocolo SNMP v3;
- 2.1.4.2.44. Prover mecanismo de realização automática de backup de toda a configuração do Equipamento de segurança, incluindo os módulos de firewall (item 2.1) e a própria solução de gerenciamento;
- 2.1.4.2.45. Possuir capacidade de carregar qualquer backup realizado anteriormente pelo sistema automático de backup descrito anteriormente;
- 2.1.4.2.46. Permitir a verificação da utilização ("hit counts") de cada regra de filtragem ("Access Control Entry") individualmente, independentemente do fato de a configuração da política ter utilizado o conceito de agrupamento lógico de objetos.

## **2.2. ITEM II – FIREWALL/VSX – CONFIGURAÇÃO I**

2.2.1. Aquisição de solução integrada de firewall virtual, com gerência e VPN com as seguintes características gerais:

2.2.1.1. A solução contemplará o fornecimento de Cluster de Firewall virtual, gerência e VPN, proporcionando maior segurança e controle do tráfego de rede no Serpro. A solução deverá ser instalada com base na topologia de rede do Serpro.

2.2.1.2. A solução proposta contemplará o fornecimento de equipamentos redundantes proporcionando alta disponibilidade. Diante da falha ou indisponibilidade de qualquer um dos equipamentos ou componentes, o(s) remanescente(s) deverá(ão) assumir de forma imediata, não acarretando interrupções no tráfego de rede e mantendo o desempenho mínimo especificado nos itens 2.2.1.3.1 ao 2.2.1.3.6. Além da alta disponibilidade, a solução possibilitará o balanceamento interno de carga, distribuindo as conexões entre os equipamentos, melhorando o desempenho no acesso e possibilitando uma melhor utilização da solução.

### **2.2.1.3. Características de hardware**

2.2.1.3.1. A solução deverá ser entregue em ambiente de cluster com no mínimo 2 (dois) appliances físicos;

2.2.1.3.2. Permitir 300.000 (trezentos mil) conexões por segundo (CPS); (AMOSTRA)

- 2.2.1.3.3. Permitir 4.500.000 (quatro milhões e quinhentos mil) pacotes por segundo (PPS); (AMOSTRA)
- 2.2.1.3.4. Permitir 3.300.000 (três milhões e trezentos mil) conexões simultâneas;
- 2.2.1.3.5. Capacidade para suportar Throughput de 10 Gbps de VPN;
- 2.2.1.3.6. Capacidade para suportar Throughput de 20 Gbps de tráfego inspecionado para Firewall, usando-se como base o padrão IMIX (57% de pacotes de 64bytes, 23% de pacotes de 570bytes e 20% de pacotes de 1518bytes);(AMOSTRA)
- 2.2.1.3.7. Os hardwares ofertados deverão ser do tipo appliance, desenvolvidos para as funcionalidades de Firewall, VPN e gerência;
- 2.2.1.3.8. Cada appliance de Firewall deve ser fornecido com, no mínimo, 8 (oito) interfaces de 10 Gigabit Ethernet padrão SFP+ e 12 (doze) interfaces Gigabit Ethernet 1000Mbps para cabeamento de cobre, com possibilidade de expansão por módulos. As interfaces de rede devem ser todas frontais;
- 2.2.1.3.9. As faixas de tensão de entrada suportadas devem ser de 100 VAC a 127 VAC e de 200 VAC a 240 VAC, a 60 Hz sem uso de chave de seleção de voltagem (automaticamente), capaz de sustentar a configuração máxima do servidor;
- 2.2.1.3.10. Os appliances e gerências devem ser fornecidos com fontes internas ou externas com tolerância a falha e capacidade de liga-se em 2 circuitos de alimentação diferentes; (AMOSTRA)

#### **2.2.1.4. Características do software de firewall**

- 2.2.1.4.1. Permitir que backups de configuração e logs sejam armazenados;
- 2.2.1.4.2. A solução de Firewall e gerência deverão suportar restauração dos sistemas neles instalados a partir de um backup prévio;
- 2.2.1.4.3. Permitir que os backups sejam transferidos para um servidor via SCP ou FTP;
- 2.2.1.4.4. A licença de uso não faz restrição para o número de usuários que use ou se comunique com o sistema de segurança;
- 2.2.1.4.5. Todos os softwares devem estar instalados e licenciados para este tipo de uso;
- 2.2.1.4.6. A solução de Firewall deve funcionar em cluster do tipo ativo-standby ou ativo-ativo com o balanceamento interno; (AMOSTRA)
- 2.2.1.4.7. Os appliances de firewall devem possibilitar acesso administrativo via protocolo seguro;
- 2.2.1.4.8. Possuir suporte a tecnologia de Firewall Virtual, sendo fornecido com pelo menos 20 (vinte) contextos por cluster, totalmente isoladas entre si. Dentro de cada instância de Firewall deve ser possível definir, independentemente de outras instâncias, regras de filtragem, regras de NAT, rotas e VLANs alocadas;
- 2.2.1.4.9. Dentro de cada instância de Firewall deve ser possível alocar o número de conexões simultâneas e estabelecimento de novas conexões por segundo; (AMOSTRA)
- 2.2.1.4.10. A exaustão dos recursos alocados para uma dada instância de Firewall não deve ter influência sobre a operação das demais instâncias;
- 2.2.1.4.11. A contratada será responsável pela migração integral das políticas, regras, NATs, rotas, objetos e demais parâmetros que se façam necessários para a reprodução completa do cenário operacional para a nova solução, que configura a “implantação total” da solução, nas regionais de Brasília, São Paulo e Rio de Janeiro. O volume atual de objetos de rede a serem migrados é da ordem de, aproximadamente, 9000 para Brasília, 4000 para São Paulo, 4000 para o Rio de Janeiro.
- 2.2.1.4.12. Suportar o protocolo DHCP no modo relay;
- 2.2.1.4.13. Suportar H.323 V2, 3 e 4; H.225 v2, 3 e 4; H.245 ; NAT para H.323;
- 2.2.1.4.14. Suportar SNMP v3;
- 2.2.1.4.15. Suportar esquemas de VPN site-to-site e client-to-site;
- 2.2.1.4.16. Fornecer criptografia e autenticação de pacotes IP, com chaves de criptografia de, 3DES/AES, no mínimo, de forma a possibilitar a criação de canais seguros ou IPSEC VPNs;
- 2.2.1.4.17. Ter compatibilidade com o padrão IPSEC, de acordo com as RFCs 2401 a 2412, de modo a estabelecer canais de criptografia com outros produtos que também suportem tal padrão;



- 2.2.1.4.18. Possuir a capacidade de alertar os administradores através de e-mail, por meio do protocolo SNMP ou scripts e executáveis definidos pelos administradores sobre os eventos de segurança gerados no firewall;
- 2.2.1.4.19. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma determinada comunicação deve ter origem;
- 2.2.1.4.20. Prover mecanismo contra ataques de negação de serviço (DoS) e SYN Flood, repassando somente as conexões estabelecidas entre os segmentos;
- 2.2.1.4.21. Suportar inspeção stateful de tráfego IPv4 e IPv6;
- 2.2.1.4.22. Suportar simultaneamente a criação de regras IPv4 e IPv6;
- 2.2.1.4.23. Suportar roteamento estático de tráfego IPv6;
- 2.2.1.4.24. Suportar anti-spoofing (sem uso de ACLs) para endereços IPv4 e IPv6;
- 2.2.1.4.25. Suportar gerenciamento sobre IPv4 e IPv6 com criptografia;
- 2.2.1.4.26. Suportar stateful failover de conexões Ipv6, sem que haja prejuízo do funcionamento das demais especificações;
- 2.2.1.4.27. Possibilidade de implementação de contexto de firewall tanto em modo transparente como também em modo gateway (roteado);
- 2.2.1.4.28. Suportar agrupamento lógico de objetos IPv6 (redes, hosts, serviços) e criação de regras (ACLs) usando tais objetos;
- 2.2.1.4.29. Suportar topologias de cluster em alta disponibilidade, de forma que em caso de indisponibilidade de um dos membros, todas as conexões ativas serão direcionadas de forma transparente para o membro ativo; (AMOSTRA)
- 2.2.1.4.30. Suportar protocolo Syslog para geração de logs de sistema;
- 2.2.1.4.31. Possuir uma ferramenta de captura de pacotes; (AMOSTRA)
- 2.2.1.4.32. O sistema operacional deverá ser customizado pelo próprio fabricante do firewall para garantir segurança e melhor performance ao firewall, permitindo o monitoramento de recursos no appliance;
- 2.2.1.4.33. Deve permitir que os diferentes contextos consigam se comunicar num mesmo domínio de broadcast, dentro da mesma estrutura de virtualização; (AMOSTRA)
- 2.2.1.4.34. Suportar a suportar o anúncio de um endereço IP virtual;
- 2.2.1.4.35. Deve permitir a criação de rotas estáticas e suportar OSPF ou BGP;
- 2.2.1.4.36. Deve suportar a definição de VLAN no firewall conforme padrão IEEE 802.1q e ser possível criar pelo menos 1024 (mil e vinte e quatro) interfaces ou subinterfaces lógicas associadas a VLANs e estabelecer regras de filtragem (Stateful Firewall) entre elas;
- 2.2.1.4.37. Deve ser possível a utilização de TAG de VLAN até 4096; (AMOSTRA)
- 2.2.1.4.38. Suportar a configuração de agregação de interfaces, conforme padrão 802.3ad;
- 2.2.1.4.39. Realizar NAT estático (1-1), dinâmico (N-1), NAT pool (N-N) e NAT condicional, possibilitando que um endereço tenha mais de um NAT dependendo da origem, destino ou porta; (AMOSTRA)
- 2.2.1.4.40. As regras de filtragem devem ter capacidade de implementação de CIDR/VLSM;
- 2.2.1.4.41. Promover a integração com diretórios LDAP (X.500) e Active Directory para a autenticação de usuários de VPN e outras demais regras de acesso, de modo que o Firewall possa utilizar das informações armazenadas para realizar autenticações;
- 2.2.1.4.42. Suportar os seguintes esquemas de autenticação de usuários por VPN: usuário e senha em base do próprio sistema de Firewall, diretório LDAP, certificação digital por meio de certificados emitidos por Autoridade Certificadora no padrão ICP-Brasil com suporte para SHA-1 e SHA-2;
- 2.2.1.4.43. Deve ser possível atuar como cliente NTP (Network Time Protocol), conforme RFC 1305, contemplando autenticação MD5 entre os peers;
- 2.2.1.4.44. Deve ser capaz de construir registro de fluxos de dados relativos a cada sessão iniciada armazenando para cada uma destas sessões informações tais como: endereços (IPv4 e IPv6) de origem e destino dos pacotes, traduções NAT, portas TCP e UDP de origem e destino, facilitando assim o controle de todo tráfego que passa ou é negado pelo Firewall e aplicação da política de segurança; (AMOSTRA)
- 2.2.1.4.45. Deve ser capaz de aplicar novas regras sem provocar indisponibilidade de serviço,

isto é, permitindo que conexões ativas ou pendentes não sofram descontinuidade no sistema de firewall; (AMOSTRA)

#### **2.2.1.5. Solução de Gerenciamento Centralizado de Firewalls**

2.2.1.5.1. Deverá ser fornecida solução de Gerência Centralizada, redundantes entre si, com licenças de sistema operacional necessárias para o correto funcionamento de cada solução de gerência centralizada;

##### **2.2.1.5.2. Características mínimas exigidas do hardware**

2.2.1.5.2.1. Deverão ser fornecidos em equipamentos dedicados (servidor ou appliance), capazes de gerenciar todos os contextos de firewall previstos nas soluções adquiridas;

2.2.1.5.2.2. Cada equipamento deve possuir capacidade de armazenamento interno de 8 terabytes com redundância, além de possuir porta para conexão com rede SAN;

2.2.1.5.2.3. A solução de console deverá possuir quantidade de memória e processamento mínima suficiente para atendimento de todas as funcionalidades e desempenho solicitados neste documento;

2.2.1.5.2.4. Deverá possuir, no mínimo 03 (três) TB de armazenamento local ou externo, em disco com pelo menos 10K RPM e que poderá ser externo ao equipamento de gerência; (AMOSTRA)

2.2.1.5.2.5. Os discos da Solução de armazenamento deverão possuir redundância em RAID 5 ou 6 via hardware, poderá ser externo ao equipamento de gerência; (AMOSTRA)

2.2.1.5.2.6. Possuir 2 (duas) placas EMULEX, QLOGIC, BROCADE, ou compatível, padrão Fibre Channel Short Wave, que poderá estar disponível no equipamento de gerência ou no equipamento de storage fornecido externamente e que possibilite a conexão aos ambientes de armazenamento da CONTRATANTE conforme tecnologia disponível no tipo de placa definido neste item e deverá ter as seguintes características:

2.2.1.5.2.6.1. Conector tipo LC;

2.2.1.5.2.6.2. Velocidade de transferência de 8Gb/s e permita ligações de 2Gb/s, 4Gb/s e 8Gb/s;

2.2.1.5.2.6.3. Suporte a Fibre Channel classes 2 ou 3;

2.2.1.5.2.6.4. Suporte a balanceamento de carga de I/O;

2.2.1.5.2.6.5. Suportar implementação a tolerância a falhas (Failover) de forma automática;

2.2.1.5.2.6.6. Não serão aceitas placas padrão Fibre Channel short wave instaladas em slots inferiores a PCI-Express x8;

2.2.1.5.2.6.7. Não serão consideradas para efeitos de somatório das quantidades mínimas exigidas, controladoras Fibre Channel instaladas “on-board”;

2.2.1.5.2.6.8. Possuir pelo menos 3 (três) portas Fibre Channel no conjunto das duas placas solicitadas;

2.2.1.5.2.6.9. A Solução deverá possuir fontes redundantes internas do tipo “Hot-swap/Hot-plug”, com capacidade para suportar toda a solução, sem perda de capacidade ou funcionalidade, no caso de falha das fontes principais; (AMOSTRA)

2.2.1.5.2.6.10. Todas as licenças de software necessárias para a ativação, da console de gerência com redundância, devem ser entregues junto com os equipamentos, não podendo ser OEM.

##### **2.2.1.5.3. Características do software de gerenciamento e administração**

2.2.1.5.3.1. Permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras em todos os clusters e contextos firewall;

2.2.1.5.3.2. Permitir a criação e aplicação de políticas “globais”, de forma centralizada, que possam ser distribuídas para todos os contextos de firewalls;

2.2.1.5.3.3. Suportar o gerenciamento de objetos de rede para utilização em regras de acesso. Deve ser possível criar, no mínimo, os seguintes tipos de objetos: hosts, gateways, firewalls, clusters, redes, faixas de endereços, NAT, usuários, VPNs. Deverá ainda permitir detectar se e onde, na base de regras, está sendo utilizado determinado objeto de rede; (AMOSTRA)

- 2.2.1.5.3.4. O licenciamento e o software não devem limitar o número de objetos, regras de segurança, NAT, endereços IP e usuários de VPN SSL;
- 2.2.1.5.3.5. Suportar agrupamento lógico de objetos (“object grouping”) para criação de regras de filtragem;
- 2.2.1.5.3.6. Possibilitar a especificação de política por tempo, ou seja, permitir a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora); (AMOSTRA)
- 2.2.1.5.3.7. A solução de gerenciamento deve suportar pelo menos 20 (vinte) contextos de firewall por site. Deve ser possível configurar de forma gráfica pelo menos a solução de Firewall provida pelo fabricante desta solução;
- 2.2.1.5.3.8. Implementar o gerenciamento simultâneo de no mínimo 10 contextos de firewall com acesso privilegiado; (AMOSTRA)
- 2.2.1.5.3.9. Implementar a contabilização das Regras de Controle de Acesso aplicadas aos contextos por ela gerenciados;
- 2.2.1.5.3.10. A solução deve permitir o agrupamento lógico de dispositivos físicos, de acordo com a funcionalidade e com a localização física dos mesmos, permitindo o gerenciamento simultâneo de vários elementos;
- 2.2.1.5.3.11. Permitir a reutilização de objetos lógicos em várias políticas de Segurança; (AMOSTRA)
- 2.2.1.5.3.12. Permitir o retorno emergencial às configurações anteriores dos dispositivos, para a necessidade de recuperação de falhas (“Rollback de configuração”);
- 2.2.1.5.3.13. Permitir distribuição centralizada de pacotes de atualização;
- 2.2.1.5.3.14. A solução deve ser capaz de testar a conectividade dos equipamentos gerenciados e contextos de firewall;
- 2.2.1.5.3.15. Suportar configuração das funcionalidades de alta disponibilidade dos dispositivos físicos e dos contextos de firewall;
- 2.2.1.5.3.16. Permitir a visualização de qual parte da topologia gerenciada (origem, destino, serviço) está sendo afetada por determinada regra;
- 2.2.1.5.3.17. Permitir a detecção de alteração e tentativas de alteração da configuração dos dispositivos físicos e contextos de firewall e avisar o administrador (acessos que não usem a interface gráfica de gerência provida pela ferramenta);
- 2.2.1.5.3.18. Prover funcionalidade para análise e auditoria de regras com capacidade de detectar regras conflitantes, regras equivalentes ou um conjunto de regras que possa ser condensado em uma única regra que venha a produzir o mesmo efeito lógico no que concerne a Políticas de Segurança;
- 2.2.1.5.3.19. Suportar operação em modo de “workflow”, ou seja, permitir que as regras sejam aplicadas somente após passar por um fluxo de aprovação gerencial;
- 2.2.1.5.3.20. Suportar acesso baseado em perfil de usuário com as permissões de visualizar, modificar, aprovar e distribuir por tipo de objeto e política;
- 2.2.1.5.3.21. Deve ser possível definir os perfis de acesso à solução (“Role Based Access Control” = RBAC) no sistema de Gerência de Controle de Acesso fornecido;
- 2.2.1.5.3.22. Suportar a configuração de VPN dos tipos “site-to-site” e “client-to-site”;
- 2.2.1.5.3.23. Permitir a identificação e exclusão de regras e objetos que estão aplicadas nos dispositivos, mas não afetam o desempenho e a segurança da rede (regras e objetos em desuso sob o ponto de vista lógico);
- 2.2.1.5.3.24. A solução de Cluster de Firewall e gerência devem suportar protocolo de autenticação para controle do acesso administrativo ao equipamento que possua pelo menos as seguintes características:
- 2.2.1.5.3.24.1. Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega;
- 2.2.1.5.3.24.2. Cifrar todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;
- 2.2.1.5.3.24.3. Registrar os comandos executados por um dado usuário e as eventuais tentativas não autorizadas de execução de comandos (accounting);
- 2.2.1.5.3.24.4. Permitir atribuição de perfis incluindo: usuário (somente leitura),

administradores e monitores com níveis de permissão diferenciados;

2.2.1.5.3.25. Possibilitar o gerenciamento (incluindo a criação, alteração, monitoração e exclusão) de objetos de rede. Os tipos de objetos deverão permitir especificar de forma distinta recurso tais como: Hosts, Gateways, Firewalls, Clusters (alta-disponibilidade), Redes, Faixas de endereços, NAT, Usuários, Agrupamento de objetos e VPNs;

2.2.1.5.3.26. Os softwares utilizados para acessar as gerências e realizar tarefas administrativas (GUI clients) deverão ser compatíveis com o sistema operacional Linux.

2.2.1.5.3.26.1. Caso não haja tal compatibilidade, deverão ser fornecidas 03 (três) licenças para o sistema operacional proprietário, uma para cada site, que permitam o acesso simultâneo de até 10 (dez) usuários distintos por localidade.

## **2.2.2. ITEM II – FIREWALL/VSX – CONFIGURAÇÃO II**

2.2.2.1. A solução contemplará o fornecimento de Cluster de Firewall virtual, gerência e VPN, proporcionando maior segurança e controle do tráfego de rede no Serpro. A solução deverá ser instalada com base na topologia de rede do Serpro;

2.2.2.2. A solução proposta contemplará o fornecimento de equipamentos redundantes proporcionando alta disponibilidade. Diante da falha ou indisponibilidade de qualquer um dos equipamentos ou componentes, o(s) remanescente(s) deverá(ão) assumir de forma imediata, não acarretando interrupções no tráfego de rede e mantendo o desempenho mínimo especificado nos itens 2.2.2.3.1 ao 2.2.2.3.6. Além da alta disponibilidade, a solução possibilitará o balanceamento interno de carga, distribuindo as conexões entre os equipamentos, melhorando o desempenho no acesso e possibilitando uma melhor utilização da solução.

### **2.2.2.3. Características de hardware**

2.2.2.3.1. A solução deverá ser entregue em ambiente de cluster com no mínimo 2 (dois) appliances físicos;

2.2.2.3.2. Permitir 150.000 (cento e cinquenta mil) conexões por segundo (CPS); (AMOSTRA)

2.2.2.3.3. Permitir 2.200.000 (dois milhões e duzentos mil) pacotes por segundo (PPS); (AMOSTRA)

2.2.2.3.4. Permitir 1.500.000 (um milhão e quinhentos mil) conexões simultâneas;

2.2.2.3.5. Capacidade para suportar Throughput de 10 Gbps de VPN;

2.2.2.3.6. Capacidade para suportar Throughput de 20 Gbps de tráfego inspecionado para Firewall, usando-se como base o padrão IMIX (57% de pacotes de 64bytes, 23% de pacotes de 570bytes e 20% de pacotes de 1518bytes); (AMOSTRA)

2.2.2.3.7. Os hardwares ofertados deverão ser do tipo appliance, desenvolvidos para as funcionalidades de Firewall, VPN e gerência;

2.2.2.3.8. Cada appliance de Firewall deve ser fornecido com, no mínimo, 8 (oito) interfaces de 10 Gigabit Ethernet padrão SFP+ e 12 (doze) interfaces Gigabit Ethernet 1000Mbps para cabeamento de cobre, com possibilidade de expansão por módulos. As interfaces de rede devem ser todas frontais;

2.2.2.3.9. As faixas de tensão de entrada suportadas devem ser de 100 VAC a 127 VAC e de 200 VAC a 240 VAC, a 60 Hz sem uso de chave de seleção de voltagem (automaticamente), capaz de sustentar a configuração máxima do servidor;

2.2.2.3.10. Os appliances e gerências devem ser fornecidos com fontes internas ou externas com tolerância a falha e capacidade de liga-se em 2 circuitos de alimentação diferentes. (AMOSTRA)

### **2.2.2.4. Características do software de firewall**

2.2.2.4.1. Permitir que backups de configuração e logs sejam armazenados;

2.2.2.4.2. A solução de Firewall e gerência deverão suportar restauração dos sistemas neles instalados a partir de um backup prévio;

2.2.2.4.3. Permitir que os backups sejam transferidos para um servidor via SCP ou FTP;

2.2.2.4.4. A licença de uso não faz restrição para o número de usuários que use ou se comunique com o sistema de segurança;

- 2.2.2.4.5. Todos os softwares devem estar instalados e licenciados para este tipo de uso;
- 2.2.2.4.6. A solução de Firewall deve funcionar em cluster do tipo ativo-standby ou ativo-ativo com o balanceamento interno; (AMOSTRA)
- 2.2.2.4.7. Os appliances de firewall devem possibilitar acesso administrativo via protocolo seguro;
- 2.2.2.4.8. Possuir suporte a tecnologia de Firewall Virtual, sendo fornecido com pelo menos 20 (vinte) contextos por cluster, totalmente isoladas entre si. Dentro de cada instância de Firewall deve ser possível definir, independentemente de outras instâncias, regras de filtragem, regras de NAT, rotas e VLANs alocadas;
- 2.2.2.4.9. Dentro de cada instância de Firewall deve ser possível alocar o número de conexões simultâneas e estabelecimento de novas conexões por segundo; (AMOSTRA)
- 2.2.2.4.10. A exaustão dos recursos alocados para uma dada instância de Firewall não deve ter influência sobre a operação das demais instâncias;
- 2.2.2.4.11. A contratada será responsável pela migração integral das políticas, regras, NATs, rotas, objetos e demais parâmetros que se façam necessários para a reprodução completa do cenário operacional para a nova solução, que configura a “implantação total” da solução, nas regionais de Brasília, São Paulo e Rio de Janeiro. O volume atual de objetos de rede a serem migrados é da ordem de, aproximadamente, 9.000 para Brasília, 4.000 para São Paulo, 4.000 para o Rio de Janeiro;
- 2.2.2.4.12. Suportar o protocolo DHCP no modo relay;
- 2.2.2.4.13. Suportar H.323 V2, 3 e 4; H.225 v2, 3 e 4; H.245 ; NAT para H.323;
- 2.2.2.4.14. Suportar SNMP v3;
- 2.2.2.4.15. Suportar esquemas de VPN site-to-site e client-to-site;  
Fornecer criptografia e autenticação de pacotes IP, com chaves de criptografia de, 3DES/AES, no mínimo, de forma a possibilitar a criação de canais seguros ou IPSEC VPNs;
- 2.2.2.4.16. Compatibilidade com o padrão IPSEC, de acordo com as RFCs 2401 a 2412, de modo a estabelecer canais de criptografia com outros produtos que também suportem tal padrão;
- 2.2.2.4.17. Possuir a capacidade de alertar os administradores através de e-mail, por meio do protocolo SNMP ou scripts e executáveis definidos pelos administradores sobre os eventos de segurança gerados no firewall;
- 2.2.2.4.18. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma determinada comunicação deve ter origem;
- 2.2.2.4.19. Prover mecanismo contra ataques de negação de serviço (DoS) e SYN Flood, repassando somente as conexões estabelecidas entre os segmentos;
- 2.2.2.4.20. Suportar inspeção stateful de tráfego IPv4 e IPv6;
- 2.2.2.4.21. Suportar simultaneamente a criação de regras IPv4 e IPv6;
- 2.2.2.4.22. Suportar roteamento estático de tráfego IPv6;
- 2.2.2.4.23. Suportar anti-spoofing (sem uso de ACLs) para endereços IPv4 e IPv6;
- 2.2.2.4.24. Suportar gerenciamento sobre IPv4 e IPv6 com criptografia;
- 2.2.2.4.25. Suportar stateful failover de conexões Ipv6, sem que haja prejuízo do funcionamento das demais especificações;
- 2.2.2.4.26. Possibilidade de implementação de contexto de firewall tanto em modo transparente como também em modo gateway; (roteado)
- 2.2.2.4.27. Suportar agrupamento lógico de objetos IPv6 (redes, hosts, serviços) e criação de regras (ACLs) usando tais objetos;
- 2.2.2.4.28. Suportar topologias de cluster em alta disponibilidade, de forma que em caso de indisponibilidade de um dos membros, todas as conexões ativas serão direcionadas de forma transparente para o membro ativo; (AMOSTRA)
- 2.2.2.4.29. Suportar protocolo Syslog para geração de logs de sistema;
- 2.2.2.4.30. Possuir uma ferramenta de captura de pacotes; (AMOSTRA)
- 2.2.2.4.31. O sistema operacional deverá ser customizado pelo próprio fabricante do firewall para garantir segurança e melhor performance ao firewall, permitindo o monitoramento de recursos no appliance;

- 2.2.2.4.32. Deve permitir que os diferentes contextos consigam se comunicar num mesmo domínio de broadcast, dentro da mesma estrutura de virtualização. (AMOSTRA)
- 2.2.2.4.33. Suportar a suportar o anúncio de um endereço IP virtual;
- 2.2.2.4.34. Deve permitir a criação de rotas estáticas e suportar OSPF ou BGP;
- 2.2.2.4.35. Deve suportar a definição de VLAN no firewall conforme padrão IEEE 802.1q e ser possível criar pelo menos 1024 (mil e vinte e quatro) interfaces ou subinterfaces lógicas associadas a VLANs e estabelecer regras de filtragem (Stateful Firewall) entre elas;
- 2.2.2.4.36. Deve ser possível a utilização de TAG de VLAN até 4096; (AMOSTRA)
- 2.2.2.4.37. Suportar a configuração de agregação de interfaces, conforme padrão 802.3ad;
- 2.2.2.4.38. Realizar NAT estático (1-1), dinâmico (N-1), NAT pool (N-N) e NAT condicional, possibilitando que um endereço tenha mais de um NAT dependendo da origem, destino ou porta; (AMOSTRA)
- 2.2.2.4.39. As regras de filtragem devem ter capacidade de implementação de CIDR/VLSM;
- 2.2.2.4.40. Promover a integração com diretórios LDAP (X.500) e Active Directory para a autenticação de usuários de VPN e outras demais regras de acesso, de modo que o Firewall possa utilizar das informações armazenadas para realizar autenticações;
- 2.2.2.4.41. Suportar os seguintes esquemas de autenticação de usuários por VPN: usuário e senha em base do próprio sistema de Firewall, diretório LDAP, certificação digital por meio de certificados emitidos por Autoridade Certificadora no padrão ICP-Brasil com suporte para SHA-1 e SHA-2;
- 2.2.2.4.42. Deve ser possível atuar como cliente NTP (Network Time Protocol), conforme RFC 1305, contemplando autenticação MD5 entre os peers;
- 2.2.2.4.43. Deve ser capaz de construir registro de fluxos de dados relativos a cada sessão iniciada armazenando para cada uma destas sessões informações tais como: endereços (IPv4 e IPv6) de origem e destino dos pacotes, traduções NAT, portas TCP e UDP de origem e destino, facilitando assim o controle de todo tráfego que passa ou é negado pelo Firewall e aplicação da política de segurança; (AMOSTRA)
- 2.2.2.4.44. Deve ser capaz de aplicar novas regras sem provocar indisponibilidade de serviço, isto é, permitindo que conexões ativas ou pendentes não sofram descontinuidade no sistema de firewall; (AMOSTRA)

### **2.2.2.5. Solução de Gerenciamento Centralizado de firewalls**

2.2.2.5.1. Deverão ser fornecidas três (03) soluções de Gerência Centralizada, a serem instaladas em Brasília, Rio de Janeiro e São Paulo, redundantes entre si, com licenças de sistema operacional necessárias para o correto funcionamento de cada solução de gerência centralizada.

#### **2.2.2.5.2. Características mínimas exigidas do hardware**

- 2.2.2.5.2.1. Deverão ser fornecidos em equipamentos dedicados (servidor ou appliance), capazes de gerenciar todos os contextos de firewall previstos nas soluções adquiridas;
- 2.2.2.5.2.2. Cada equipamento deve possuir capacidade de armazenamento interno de 8 terabytes com redundância, além de possuir porta para conexão com rede SAN;
- 2.2.2.5.2.3. A solução de console deverá possuir quantidade de memória e processamento mínima suficiente para atendimento de todas as funcionalidades e desempenho solicitados;
- 2.2.2.5.2.4. Possuir, no mínimo 03 (três) TB de armazenamento local ou externo, em disco com pelo menos 10K RPM e que poderá ser externo ao equipamento de gerencia; (AMOSTRA)
- 2.2.2.5.2.5. Os discos da Solução de armazenamento deverão possuir redundância em RAID 5 ou 6 via hardware, poderá ser externo ao equipamento de gerencia; (AMOSTRA)
- 2.2.2.5.2.6. Possuir 2 (duas) placas EMULEX, QLOGIC, BROCADE, ou compatível, padrão Fibre Channel Short Wave, que poderá estar disponível no equipamento de gerência ou no equipamento de storage fornecido externamente e que possibilite a conexão aos ambientes de armazenamento da CONTRATANTE conforme tecnologia disponível no tipo de placa definido neste item e deverá ter as seguintes características:
- 2.2.2.5.2.6.1. Conector tipo LC;

2.2.2.5.2.6.2. Velocidade de transferência de 8Gb/s e permita ligações de 2Gb/s, 4Gb/s e 8Gb/s;

2.2.2.5.2.6.3. Suporte a Fibre Channel classes 2 ou 3;

2.2.2.5.2.6.4. Suporte a balanceamento de carga de I/O;

2.2.2.5.2.6.5. Suportar implementação a tolerância a falhas (Failover) de forma automática;

2.2.2.5.2.6.6. Não serão aceitas placas padrão Fibre Channel short wave instaladas em slots inferiores a PCI-Express x8;

2.2.2.5.2.6.7. Não serão consideradas para efeitos de somatório das quantidades mínimas exigidas, controladoras Fibre Channel instaladas “on-board”;

2.2.2.5.2.6.8. Possuir pelo menos 3 (três) portas Fibre Channel no conjunto das duas placas solicitadas;

2.2.2.5.2.7. A Solução deverá possuir fontes redundantes internas do tipo “Hot-swap/Hot-plug”, com capacidade para suportar toda a solução, sem perda de capacidade ou funcionalidade, no caso de falha das fontes principais; (AMOSTRA)

2.2.2.5.2.8. Todas as licenças de software necessárias para a ativação da console de gerencia com redundância devem ser entregues junto com os equipamento, não podendo ser OEM;

### **2.2.2.5.2.3. Características do software de gerenciamento e administração**

2.2.2.5.2.3.1. Permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras em todos os clusters e contextos firewall;

2.2.2.5.2.3.2. Permitir a criação e aplicação de políticas “globais”, de forma centralizada, que possam ser distribuídas para todos os contextos de firewalls;

2.2.2.5.2.3.3. Suportar o gerenciamento de objetos de rede para utilização em regras de acesso. Deve ser possível criar, no mínimo, os seguintes tipos de objetos: hosts, gateways, firewalls, clusters, redes, faixas de endereços, NAT, usuários, VPNs. Deverá ainda permitir detectar se e onde, na base de regras, está sendo utilizado determinado objeto de rede; (AMOSTRA)

2.2.2.5.2.3.4. O licenciamento e o software não devem limitar o número de objetos, regras de segurança, NAT, endereços IP e usuários de VPN SSL;

2.2.2.5.2.3.5. Suportar agrupamento lógico de objetos (“object grouping”) para criação de regras de filtragem;

2.2.2.5.2.3.6. Possibilitar a especificação de política por tempo, ou seja, permitir a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora); (AMOSTRA)

2.2.2.5.2.3.7. A solução de gerenciamento deve suportar pelo menos 20 (vinte) contextos de firewall por site. Deve ser possível configurar de forma gráfica pelo menos a solução de Firewall provida pelo fabricante desta solução;

2.2.2.5.2.3.8. Implementar o gerenciamento simultâneo de no mínimo 10 contextos de firewall com acesso privilegiado; (AMOSTRA)

2.2.2.5.2.3.9. Implementar a contabilização das Regras de Controle de Acesso aplicadas aos contextos por ela gerenciados;

2.2.2.5.2.3.10. A solução deve permitir o agrupamento lógico de dispositivos físicos, de acordo com a funcionalidade e com a localização física dos mesmos, permitindo o gerenciamento simultâneo de vários elementos;

2.2.2.5.2.3.11. Permitir a reutilização de objetos lógicos em várias políticas de Segurança; (AMOSTRA)

2.2.2.5.2.3.12. Permitir o retorno emergencial às configurações anteriores dos dispositivos, para a necessidade de recuperação de falhas (“Rollback de configuração”);

2.2.2.5.2.3.13. Permitir distribuição centralizada de pacotes de atualização;

2.2.2.5.2.3.14. A solução deve ser capaz de testar a conectividade dos equipamentos gerenciados e contextos de firewall;

2.2.2.5.2.3.15. Suportar configuração das funcionalidades de alta disponibilidade dos dispositivos físicos e dos contextos de firewall;

- 2.2.2.5.2.3.16. Permitir a visualização de qual parte da topologia gerenciada (origem, destino, serviço) está sendo afetada por determinada regra;
- 2.2.2.5.2.3.17. Permitir a detecção de alteração e tentativas de alteração da configuração dos dispositivos físicos e contextos de firewall e avisar o administrador (acessos que não usem a interface gráfica de gerência provida pela ferramenta);
- 2.2.2.5.2.3.18. Prover funcionalidade para análise e auditoria de regras com capacidade de detectar regras conflitantes, regras equivalentes ou um conjunto de regras que possa ser condensado em uma única regra que venha a produzir o mesmo efeito lógico no que concerne a Políticas de Segurança;
- 2.2.2.5.2.3.19. Suportar operação em modo de “workflow”, ou seja, permitir que as regras sejam aplicadas somente após passar por um fluxo de aprovação gerencial;
- 2.2.2.5.2.3.20. Suportar acesso baseado em perfil de usuário com as permissões de visualizar, modificar, aprovar e distribuir por tipo de objeto e política;
- 2.2.2.5.2.3.21. Deve ser possível definir os perfis de acesso à solução (“Role Based Access Control” = RBAC) no sistema de Gerência de Controle de Acesso fornecido;
- 2.2.2.5.2.3.22. Suportar a configuração de VPN dos tipos “site-to-site” e “client-to-site”;
- 2.2.2.5.2.3.23. Permitir a identificação e exclusão de regras e objetos que estão aplicadas nos dispositivos, mas não afetam o desempenho e a segurança da rede (regras e objetos em desuso sob o ponto de vista lógico);
- 2.2.2.5.2.3.24. A solução de Cluster de Firewall e gerência devem suportar protocolo de autenticação para controle do acesso administrativo ao equipamento que possua pelo menos as seguintes características:**
- 2.2.2.5.2.3.24.1. Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega;
- 2.2.2.5.2.3.24.2. Cifrar todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;
- 2.2.2.5.2.3.24.3. Registrar os comandos executados por um dado usuário e as eventuais tentativas não autorizadas de execução de comandos (accounting);
- 2.2.2.5.2.3.24.4. Permitir atribuição de perfis incluindo: usuário (somente leitura), administradores e monitores com níveis de permissão diferenciados.
- 2.2.2.5.2.3.25. Possibilitar o gerenciamento (incluindo a criação, alteração, monitoração e exclusão) de objetos de rede. Os tipos de objetos deverão permitir especificar de forma distinta recurso tais como: Hosts, Gateways, Firewalls, Clusters (alta-disponibilidade), Redes, Faixas de endereços, NAT, Usuários, Agrupamento de objetos e VPNs;
- 2.2.2.5.2.3.26. Os softwares utilizados para acessar as gerências e realizar tarefas administrativas (GUI clients) deverão ser compatíveis com o sistema operacional Linux.
- 2.2.2.5.2.3.26.1. Caso não haja tal compatibilidade, deverão ser fornecidas 03 (três) licenças para o sistema operacional proprietário, uma para cada site, que permitam o acesso simultâneo de até 10 (dez) usuários distintos por localidade.

## **2.2.3. ITEM III – FIREWALLS AMBIENTES DE SERVIÇOS INTERNOS: SEGMENTAÇÃO, REGIONAIS e VPN**

### **2.2.3.1. CONFIGURAÇÃO I – FIREWALLS INTERNOS REGIONAIS**

A solução contemplará o fornecimento de cluster de Firewall proporcionando maior segurança e controle do tráfego de rede no Serpro. A solução deverá ser instalada com base na topologia de rede do Serpro.

#### **2.2.3.1.1. Características de hardware por equipamento**

- 2.2.3.1.1.1. O hardware ofertado deverá ser do tipo appliance, desenvolvido para as funcionalidades de Firewall e terminação de VPNs;
- 2.2.3.1.1.2. Sistema de segurança composto de Firewall e VPN IPSEC, o software deve estar pré-instalado;
- 2.2.3.1.1.3. A solução deve funcionar em cluster do tipo ativo-standby/Ativo-ativo com o balanceamento interno;
- 2.2.3.1.1.4. Todos os softwares, da solução, devem estar instalados e licenciados para este



tipo de uso. Ambos os dispositivos do cluster devem ser fornecidos;

2.2.3.1.1.5. O appliance deve possibilitar acesso via SSH e interface Web via HTTPS;

2.2.3.1.1.6. O appliance deve suportar restore dos sistemas instalados no appliance;

2.2.3.1.1.7. Permitir que backups de configuração sejam armazenados;

2.2.3.1.1.8. Permitir que os backups sejam transferidos para um servidor via SCP ou FTP;

2.2.3.1.1.9. Deve ser fornecido com, no mínimo, 8 (oito) interfaces de rede Gigabit Ethernet 1000Mbps;

2.2.3.1.1.10. Possuir 02 (duas) fontes de alimentação independentes e redundantes, com tensão de entrada de 120V a 240V AC (manual ou automática), e frequência de 60Hz;

2.2.3.1.1.11. Capacidade para suportar Throughput de 5 Gbps de tráfego inspecionado para Firewall, usando-se como base o padrão IMIX (57% de pacotes de 64bytes, 23% de pacotes de 570bytes e 20% de pacotes de 1518bytes); (AMOSTRA)

2.2.3.1.1.12. Deve possuir throughput mínimo de 3 (três) GB para tráfego de VPN, considerando-se os padrões criptográficos 3DES e AES;

2.2.3.1.1.13. Deve possuir suporte para no mínimo 1.000.000 (um milhão) sessões TCP concorrentes;

2.2.3.1.1.14. Cada appliance deve possuir capacidade de suportar no mínimo 80.000 (oitenta mil) novas sessões TCP por segundo;

2.2.3.1.1.15. Suportar encaminhamento de pelo menos 1.500.000 (um milhão e quinhentos mil) pacotes por segundo (pps);

2.2.3.1.1.16. Deve suportar a definição de VLAN no firewall conforme padrão IEEE 802.1q e ser possível criar pelo menos 1024 (mil e vinte e quatro) interfaces ou subinterfaces lógicas associadas a VLANs e estabelecer regras de filtragem (Stateful Firewall) entre elas.

2.2.3.1.1.17. Deve ser possível a utilização de TAG de VLAN até 4096;

#### **2.2.3.1.2. Características do Software de Firewall/Vpn**

2.2.3.1.2.1. A licença de uso não faz restrição para o número endereços que use ou se comunique com o sistema de segurança;

2.2.3.1.2.2. Possibilidade de implementação em modo transparente e gateway;

2.2.3.1.2.3. Suportar as tecnologias de rede: Ethernet, Fast Ethernet e Gigabit Ethernet;

2.2.3.1.2.5. Suportar DHCP relay;

2.2.3.1.2.6. Promover a integração com diretórios LDAP para a autenticação de usuários, de modo que o Firewall possa utilizar das informações armazenadas para realizar autenticações;

2.2.3.1.2.7. Permitir a integração com qualquer Autoridade Certificadora emissora de certificados X.509 que seguir o padrão de PKI (descrito na RFC 2459), inclusive verificando as CRLs (Listas de Certificados Revogados) emitidas periodicamente pelas Autoridades Certificadoras, que devem ser obtidas automaticamente pelo firewall via protocolo HTTP ou LDAP;

2.2.3.1.2.8. Suportar H.323 V2, 3 e 4; H.225 v2, 3 e 4; H.245 ; NAT para H.323;

2.2.3.1.2.9. Realizar NAT estático (1-1) e dinâmico (N-1);

2.2.3.1.2.10. Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, Real Áudio, Real Vídeo e RTSP, SIP, H323, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para tráfego outbound (de dentro para fora) quanto inbound (de fora para dentro);

2.2.3.1.2.11. Suportar topologias de cluster em alta disponibilidade e/ou em balanceamento de tráfego entre dois ou mais equipamentos de Firewall, de forma que em caso de indisponibilidade de um dos membros, todas as conexões ativas serão direcionadas de forma transparente para o membro ativo;

2.2.3.1.2.12. Suportar inspeção stateful de tráfego Ipv6;

2.2.3.1.2.13. Deve suportar agrupamento lógico de objetos de configuração ("object grouping") para criação de regras de filtragem. Deve ser possível criar grupos de pelo menos os seguintes tipos de objetos : hosts, redes IP, serviços. Deve ser possível verificar a utilização ("hit counts") de cada regra de filtragem ("Access Control Entry") individualmente, independentemente do fato de a configuração da política ter utilizado o conceito de agrupamento lógico de objetos;

- 2.2.3.1.2.14. Suportar SNMP v3;
- 2.2.3.1.2.15. Possuir Mibs SNMP V2/V3 proprietárias, para medir a quantidade de sessões simultâneas de cada túnel VPN;
- 2.2.3.1.2.16. O concentrador VPN deve suportar protocolo Syslog para geração de logs de sistema;
- 2.2.3.1.2.17. Implementar NTP (Network Time Protocol), conforme RFC 1305, contemplando autenticação MD5 entre os peers;
- 2.2.3.1.2.18. Deve ser gerenciável via porta de console, SSHv2 e HTTPS;
- 2.2.3.1.2.19. Possuir uma ferramenta de captura de pacotes;
- 2.2.3.1.2.20. Deve permitir o armazenamento de pacotes capturados em formato tcpdump;
- 2.2.3.1.2.21. Possibilitar o registro de toda a comunicação realizada através do firewall e de todas as tentativas de abertura de sessões e conexões que por ele forem recusadas;
- 2.2.3.1.2.22. Suportar a configuração de VPN tipos “site-to-site” e “client-to-site”;
- 2.2.3.1.2.23. Suportar, no mínimo, 1.000 (mil) conexões VPN IPSec qualquer combinação entre sites simultaneamente;
- 2.2.3.1.2.24. Suportar pelo menos os seguintes algoritmos de criptografia simétricos: AES256, AES128, DES, e 3DES;
- 2.2.3.1.2.25. Permitir que os gateways VPN em uma topologia site-to-site se autenticuem via pre-shared secret e certificados;
- 2.2.3.1.2.26. Suportar os algoritmos para geração de chave publica: RSA e Diffie-Hellman, abrangendo os seguintes grupos: Grupo 2 (1024 bits), Grupo 1 (768 bits), Grupo 5 (1536 bits);
- 2.2.3.1.2.27. Possuir capacidade de aumentar o desempenho de VPN através de soluções de hardware, tais como placas aceleradoras;
- 2.2.3.1.2.28. Suportar autoridade certificadora integrada ao gateway VPN;
- 2.2.3.1.2.29 Promover a integração com diretórios LDAP (X.500) e Active Directory para a autenticação de usuários de VPN e outras demais regras de acesso, de modo que o Firewall possa utilizar das informações armazenadas para realizar autenticações;
- 2.2.3.1.2.30. Suportar os seguintes esquemas de autenticação de usuários por VPN: usuário e senha em base do próprio sistema de Firewall, diretório LDAP, certificação digital por meio de certificados emitidos por Autoridade Certificadora no padrão ICP-Brasil com suporte para SHA-1 e SHA-2;
- 2.2.3.1.2.31. Suportar a integração com autoridades certificadoras de terceiros que possam gerar certificados no formato PKCS#12;
- 2.2.3.1.2.32. Suportar a solicitação de emissão de certificados à uma autoridade certificadora de confiança (enrollment) via SCEP (Simple Certificate Enrollment Protocol);
- 2.2.3.1.2.33. Suportar leitura e verificação de Lista de Certificados Revogados através de, no mínimo, HTTP e LDAP;
- 2.2.3.1.2.34. Suportar NAT-T (NAT Traversal), permitindo a utilização dos clientes VPN em ambientes em que já se efetue PAT (Port Address Translation);
- 2.2.3.1.2.35. Deve permitir a criação de rotas estáticas e suportar OSPF ou BGP;

### **2.2.3.1.3. Características do software de gerenciamento e administração**

- 2.2.3.1.3.1. Permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras em todos os clusters;
- 2.2.3.1.3.2. Suportar o gerenciamento de objetos de rede para utilização em regras de acesso. Deve ser possível criar, no mínimo, os seguintes tipos de objetos: hosts, gateways, firewalls, clusters, redes, faixas de endereços, NAT, usuários, VPNs. Deverá ainda permitir detectar se e onde, na base de regras, está sendo utilizado determinado objeto de rede.  
(AMOSTRA)
- 2.2.3.1.3.3. O licenciamento e o software não devem limitar o número de objetos, regras de segurança, NAT, endereços IP;
- 2.2.3.1.3.4. Suportar agrupamento lógico de objetos (“object grouping”) para criação de regras de filtragem;
- 2.2.3.1.3.5. Possibilitar a especificação de política por tempo, ou seja, permitir a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

(AMOSTRA)

2.2.3.1.3.6. Implementar a contabilização das Regras de Controle de Acesso por ela gerenciadas;

2.2.3.1.3.7. A solução deve permitir o agrupamento lógico de dispositivos físicos, de acordo com a funcionalidade e com a localização física dos mesmos, permitindo o gerenciamento simultâneo de vários elementos;

2.2.3.1.3.8. Permitir a reutilização de objetos lógicos em várias políticas de Segurança;

(AMOSTRA)

2.2.3.1.3.9. Permitir o retorno emergencial às configurações anteriores dos dispositivos, para a necessidade de recuperação de falhas (“Rollback de configuração”);

2.2.3.1.3.10. Permitir distribuição centralizada de pacotes de atualização;

2.2.3.1.3.11. A solução deve ser capaz de testar a conectividade dos equipamentos gerenciados;

2.2.3.1.3.12. Suportar configuração das funcionalidades de alta disponibilidade dos dispositivos físicos;

2.2.3.1.3.13. Permitir a visualização de qual parte da topologia gerenciada (origem, destino, serviço) está sendo afetada por determinada regra;

2.2.3.1.3.14. Permitir a detecção de alteração e tentativas de alteração da configuração dos dispositivos físicos;

2.2.3.1.3.15. Prover funcionalidade para análise e auditoria de regras com capacidade de detectar regras conflitantes, regras equivalentes ou um conjunto de regras que possa ser condensado em uma única regra que venha a produzir o mesmo efeito lógico no que concerne às Políticas de Segurança;

2.2.3.1.3.16. Suportar operação em modo de “workflow”, ou seja, permitir que as regras sejam aplicadas somente após passar por um fluxo de aprovação gerencial;

2.2.3.1.3.17. Suportar acesso baseado em perfil de usuário com as permissões de visualizar, modificar, aprovar e distribuir por tipo de objeto e política;

2.2.3.1.3.18. Deve ser possível definir os perfis de acesso à solução (“Role Based Access Control” = RBAC) no sistema de Gerência de Controle de Acesso fornecido;

2.2.3.1.3.19. Permitir a identificação e exclusão de regras e objetos que estão aplicadas nos dispositivos, mas não afetam o desempenho e a segurança da rede (regras e objetos em desuso sob o ponto de vista lógico);

2.2.3.1.3.20. A solução de Cluster de Firewall e Gerência devem suportar protocolos de autenticação para controle do acesso administrativo ao equipamento que possua pelo menos as seguintes características:

2.2.3.1.3.20.1. Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega;

2.2.3.1.3.20.2. Cifrar todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;

2.2.3.1.3.20.3. Registrar os comandos executados por um dado usuário e as eventuais tentativas não autorizadas de execução de comandos (accounting);

2.2.3.1.3.20.4. Permitir atribuição de perfis incluindo: usuário (somente leitura), administradores e monitores com níveis de permissão diferenciados;

2.2.3.1.3.20.5. Possibilitar o gerenciamento (incluindo a criação, alteração, monitoração e exclusão) de objetos de rede. Os tipos de objetos deverão permitir especificar de forma distinta recurso tais como: Hosts, Gateways, Firewalls, Clusters (alta-disponibilidade), Redes, Faixas de endereços, NAT, Usuários, Agrupamento de objetos e VPNs;

2.2.3.1.3.20.6. Os softwares utilizados para acessar as gerências e realizar tarefas administrativas (GUI clients) deverão ser compatíveis com o sistema operacional Linux;

2.2.3.1.3.20.6.1. Caso não haja tal compatibilidade, deverão ser fornecidas 3 (três) licenças para o sistema operacional proprietário, uma para cada site, que permitam o acesso simultâneo de até 10 (dez) usuários distintos por localidade;

2.2.3.1.3.20.7. Possuir interface gráfica capaz de exibir informações em tempo real e informações passadas (histórico), tais como throughput, número de sessões simultâneas, número de pacotes por segundo, serviços mais utilizados, uso de CPU, memória e disco,

número de túneis VPN, dentre outros.

2.2.3.1.3.20.7.1. Caso não exista nativamente, deverá ser feita mediante integração com solução de terceiros, a qual deverá ser fornecida configurada, juntamente com os licenciamentos necessários.

## **2.2.3. ITEM III – FIREWALLS AMBIENTES DE SERVIÇOS INTERNOS: SEGMENTAÇÃO, REGIONAIS e VPN**

### **2.2.3.2. CONFIGURAÇÃO II – PROJETO SEGMENTAÇÃO**

#### **2.2.3.2.1. Características de hardware por equipamento**

2.2.3.2.2. Os hardwares ofertados deverão ser do tipo appliance, desenvolvidos para as funcionalidades de Firewall e terminação de VPNs;

2.2.3.2.3. Sistema de segurança composto de Firewall e VPN IPSEC, o software deve estar pré-instalado;

2.2.3.2.4. A solução deve funcionar em cluster do tipo ativo-standby/Ativo-ativo com o balanceamento interno;

2.2.3.2.5. Todos os softwares devem estar instalados e licenciados para este tipo de uso;

2.2.3.2.5.1. Ambos os dispositivos do cluster devem ser fornecidos;

2.2.3.2.6. O appliance deve possibilitar acesso via SSH e interface Web via HTTPS;

2.2.3.2.7. O appliance deve suportar restore dos sistemas instalados no appliance;

2.2.3.2.8. Permitir que backups de configuração sejam armazenados;

2.2.3.2.9. Permitir que os backups sejam transferidos para um servidor via SCP ou FTP;

2.2.3.2.10. Deve ser fornecido com, no mínimo, 8 (oito) interfaces de rede Gigabit Ethernet 1000Mbps e 4 interfaces de rede 10 Gigabit Ethernet;

2.2.3.2.11. Possuir 02 (duas) fontes, de alimentação, independentes e redundantes, com tensão de entrada de 120V a 240V AC (manual ou automática), e frequência de 60Hz;

2.2.3.2.12. Possuir capacidade para suportar Throughput de 15 Gbps de tráfego inspecionado para Firewall, usando-se como base o padrão IMIX (57% de pacotes de 64bytes, 23% de pacotes de 570bytes e 20% de pacotes de 1518bytes); (AMOSTRA)

2.2.3.2.13. Possuir throughput mínimo de 3 (três) GB para tráfego de VPN, considerando-se os padrões criptográficos 3DES e AES;

2.2.3.2.14. Deve possuir suporte para no mínimo 2.000.000 (dois milhões) sessões TCP concorrentes;

2.2.3.2.15. Cada appliance deve possuir capacidade de suportar no mínimo 120.000 (cento e vinte mil) novas sessões TCP por segundo;

2.2.3.2.16. Suportar encaminhamento de pelo menos 3.000.000 (três milhões de pacotes por segundo (pps);

2.2.3.2.17. Deve suportar a definição de VLAN no firewall conforme padrão IEEE 802.1q e ser possível criar pelo menos 1024 (mil e vinte e quatro) interfaces ou subinterfaces lógicas associadas a VLANs e estabelecer regras de filtragem (Stateful Firewall) entre elas;

2.2.3.2.18. Possibilitar a utilização de TAG de VLAN até 4096.

#### **2.2.3.2.2. Características do Software de Firewall/Vpn**

2.2.3.2.2.1. A licença de uso não faz restrição para o número endereços que use ou se comunique com o sistema de segurança;

2.2.3.2.2.2. Possibilitar a implementação em modo transparente e gateway;

2.2.3.2.2.3. Suportar as tecnologias de rede: Ethernet, Fast Ethernet e Gigabit Ethernet;

2.2.3.2.2.4. Suportar DHCP relay;

2.2.3.2.2.5. Promover a integração com diretórios LDAP para a autenticação de usuários, de modo que o Firewall possa utilizar das informações armazenadas para realizar autenticações;

2.2.3.2.2.6. Permitir a integração com qualquer Autoridade Certificadora emissora de certificados X.509 que seguir o padrão de PKI (descrito na RFC 2459), inclusive verificando as CRLs (Listas de Certificados Revogados) emitidas periodicamente pelas Autoridades Certificadoras, que devem ser obtidas automaticamente pelo firewall via protocolo HTTP ou LDAP;

- 2.2.3.2.2.6. Suportar controle de aplicações multimídia, tais como voz sobre IP, áudio e vídeo streaming;
- 2.2.3.2.2.7. Realizar NAT estático (1-1) e dinâmico (N-1);
- 2.2.3.2.2.8. Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, Real Áudio, Real Vídeo e RTSP, SIP, H323, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para tráfego outbound (de dentro para fora) quanto inbound (de fora para dentro);
- 2.2.3.2.2.9. Suportar topologias de cluster em alta disponibilidade e/ou em balanceamento de tráfego entre dois ou mais equipamentos de Firewall, de forma que em caso de indisponibilidade de um dos membros, todas as conexões ativas serão direcionadas de forma transparente para o membro ativo;
- 2.2.3.2.2.10. Suportar inspeção stateful de tráfego Ipv6;
- 2.2.3.2.2.11. Suportar agrupamento lógico de objetos de configuração ("object grouping") para criação de regras de filtragem;
- 2.2.3.2.2.11.1. Deve ser possível criar grupos de pelo menos os seguintes tipos de objetos : hosts, redes IP, serviços;
- 2.2.3.2.2.11.2. Deve ser possível verificar a utilização ("hit counts") de cada regra de filtragem ("Access Control Entry") individualmente, independentemente do fato de a configuração da política ter utilizado o conceito de agrupamento lógico de objetos;
- 2.2.3.2.2.11.3. Suportar SNMP v3;
- 2.2.3.2.2.12. Possuir Mibs SNMP V2/V3 proprietárias, para medir a quantidade de sessões simultâneas de cada túnel VPN;
- 2.2.3.2.2.13. O concentrador VPN deve suportar protocolo Syslog para geração de logs de sistema;
- 2.2.3.2.2.14. Implementar NTP (Network Time Protocol), conforme RFC 1305, contemplando autenticação MD5 entre os peers;
- 2.2.3.2.2.15. Deve ser gerenciável via porta de console, Telnet, SSHv2 e HTTPS;
- 2.2.3.2.2.16. Deve possuir mecanismo interno de captura de pacotes;
- 2.2.3.2.2.17. Deve permitir o armazenamento de pacotes capturados em formato tcpdump;
- 2.2.3.2.2.18. Possibilitar o registro de toda a comunicação realizada através do firewall e de todas as tentativas de abertura de sessões e conexões que por ele forem recusadas;
- 2.2.3.2.2.19. Suportar esquemas de VPN site-to-site em topologias Full Meshed;
- 2.2.3.2.2.20. Suportar, no mínimo, 1.000 (mil) conexões VPN IPsec qualquer combinação entre sites simultaneamente;
- 2.2.3.2.2.21. Suportar pelo menos os seguintes algoritmos de criptografia simétricos: AES256, AES128, DES, e 3DES;
- 2.2.3.2.2.22. Permitir que os gateways VPN em uma topologia site-to-site se autenticuem via pre-shared secret e certificados;
- 2.2.3.2.2.23. Suportar os algoritmos para geração de chave pública: RSA e Diffie-Hellman, abrangendo os seguintes grupos: Grupo 2 (1024 bits), Grupo 1 (768 bits), Grupo 5 (1536 bits);
- 2.2.3.2.2.24. Possuir capacidade de aumentar o desempenho de VPN através de soluções de hardware, tais como placas aceleradoras;
- 2.2.3.2.2.25. Suportar autoridade certificadora integrada ao gateway VPN;
- 2.2.3.2.2.26. Compatibilidade com certificados digitais (PKI) de terceiros, que cumpram com o padrão X.509 v3;
- 2.2.3.2.2.27. Deverá suportar certificados digitais padrão ICP-Brasil gerados com chave de 2048 bits e algoritmo de hash SHA2 tanto para autenticação quanto para a assinatura do gateway;
- 2.2.3.2.2.28. Suportar a integração com autoridades certificadoras de terceiros que possam gerar certificados no formato PKCS#12;
- 2.2.3.2.2.29. Suportar a solicitação de emissão de certificados à uma autoridade certificadora de confiança (enrollment) via SCEP (Simple Certificate Enrollment Protocol);
- 2.2.3.2.2.30. Suportar leitura e verificação de Lista de Certificados Revogados através de, no mínimo, HTTP e LDAP;
- 2.2.3.2.2.31. Suportar NAT-T (NAT Traversal), permitindo a utilização dos clientes VPN em

ambientes em que já se efetue PAT (Port Address Translation);

2.2.3.2.2.32. Deve suportar rotas estáticas com opção para suporte a OSPF ou BGP;

### **2.2.3.2.3. Características do software de gerenciamento e administração**

2.2.3.2.3.1. Permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras em todos os clusters;

2.2.3.2.3.2. Suportar o gerenciamento de objetos de rede para utilização em regras de acesso. Deve ser possível criar, no mínimo, os seguintes tipos de objetos: hosts, gateways, firewalls, clusters, redes, faixas de endereços, NAT, usuários, VPNs. Deverá ainda permitir detectar se e onde, na base de regras, está sendo utilizado determinado objeto de rede; (AMOSTRA)

2.2.3.2.3.3. O licenciamento e o software não devem limitar o número de objetos, regras de segurança, NAT, endereços IP;

2.2.3.2.3.4. Suportar agrupamento lógico de objetos ("object grouping") para criação de regras de filtragem;

2.2.3.2.3.5. Possibilitar a especificação de política por tempo, ou seja, permitir a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora); (AMOSTRA)

2.2.3.2.3.6. Implementar a contabilização das Regras de Controle de Acesso por ela gerenciadas;

2.2.3.2.3.7. A solução deve permitir o agrupamento lógico de dispositivos físicos, de acordo com a funcionalidade e com a localização física dos mesmos, permitindo o gerenciamento simultâneo de vários elementos;

2.2.3.2.3.8. Permitir a reutilização de objetos lógicos em várias políticas de Segurança; (AMOSTRA)

2.2.3.2.3.9. Permitir o retorno emergencial às configurações anteriores dos dispositivos, para a necessidade de recuperação de falhas ("Rollback de configuração");

2.2.3.2.3.10. Permitir distribuição centralizada de pacotes de atualização;

2.2.3.2.3.11. A solução deve ser capaz de testar a conectividade dos equipamentos gerenciados;

2.2.3.2.3.11. Suportar configuração das funcionalidades de alta disponibilidade dos dispositivos físicos;

2.2.3.2.3.12. Permitir a visualização de qual parte da topologia gerenciada (origem, destino, serviço) está sendo afetada por determinada regra;

2.2.3.2.3.13. Permitir a detecção de alteração e tentativas de alteração da configuração dos dispositivos físicos;

2.2.3.2.3.14. Prover funcionalidade para análise e auditoria de regras com capacidade de detectar regras conflitantes, regras equivalentes ou um conjunto;

2.2.3.2.3.15. Suportar operação em modo de "workflow", ou seja, permitir que as regras sejam aplicadas somente após passar por um fluxo de aprovação gerencial;

2.2.3.2.3.16. Suportar acesso baseado em perfil de usuário com as permissões de visualizar, modificar, aprovar e distribuir por tipo de objeto e política;

2.2.3.2.3.17. Deve ser possível definir os perfis de acesso à solução ("Role Based Access Control" = RBAC) no sistema de Gerência de Controle de Acesso fornecido;

2.2.3.2.3.18. Suportar a configuração de VPN do tipo "site-to-site";

2.2.3.2.3.19. Permitir a identificação e exclusão de regras e objetos que estão aplicadas nos dispositivos, mas não afetam o desempenho e a segurança da rede (regras e objetos em desuso sob o ponto de vista lógico);

2.2.3.2.3.20. A solução de Cluster de Firewall e gerência devem suportar protocolo de autenticação para controle do acesso administrativo ao equipamento que possua pelo menos as seguintes características:

2.2.3.2.3.20.1. Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega;

2.2.3.2.3.20.2. Criptografar todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;

- 2.2.3.2.3.20.3. Registrar todos os comandos executados por um dado usuário na execução de comandos (accounting);
- 2.2.3.2.3.20.4. Permitir atribuição de perfis incluindo: usuário (somente leitura), administradores e monitores com níveis de permissão diferenciados;
- 2.2.3.2.3.20.5. Possibilitar o gerenciamento (incluindo a criação, alteração, monitoração e exclusão) de objetos de rede. Os tipos de objetos deverão permitir especificar de forma distinta recurso tais como: Hosts, Gateways, Firewalls, Clusters (alta-disponibilidade), Redes, Faixas de endereços, NAT, Usuários, Agrupamento de objetos e VPNs;
- 2.2.3.2.3.20.6. Os softwares utilizados para acessar as gerências e realizar tarefas administrativas (GUI clients) deverão ser compatíveis com o sistema operacional Linux;
- 2.2.3.2.3.20.6.1. Caso não haja tal compatibilidade, deverão ser fornecidas 3 (três) licenças para o sistema operacional proprietário disponibilizado.

## **2.3. ITEM III – FIREWALLS AMBIENTES DE SERVIÇOS INTERNOS: SEGMENTAÇÃO, REGIONAIS e VPN**

### **2.2.3.3. CONFIGURAÇÃO III – FIREWALLs VPN**

#### **2.2.3.3.1. Características de hardware por equipamento**

- 2.2.3.3.1.1. Os hardwares ofertados deverão ser do tipo appliance, desenvolvidos para as funcionalidades de Firewall e terminação de VPNs;
- 2.2.3.3.1.2. Sistema de segurança composto de Firewall e VPN (IPSEC e SSL), o software deve estar pré-instalado;
- 2.2.3.3.1.3. A solução deve funcionar em cluster do tipo ativo-standby/Ativo-ativo com o balanceamento interno;
- 2.2.3.3.1.4. Todos os softwares devem estar instalados e licenciados para este tipo de uso;
- 2.2.3.3.1.4.1. Ambos os dispositivos do cluster devem ser fornecidos;
- 2.2.3.3.1.5. O appliance deve possibilitar acesso via SSH e interface Web via HTTPS;
- 2.2.3.3.1.6. O appliance deve suportar restore dos sistemas instalados no appliance;
- 2.2.3.3.1.7. Permitir que backups de configuração sejam armazenados;
- 2.2.3.3.1.8. Permitir que os backups sejam transferidos para um servidor via SCP ou FTP;
- 2.2.3.3.1.9. Deve ser fornecido com, no mínimo, 8 (oito) interfaces de rede Gigabit Ethernet 1000Mbps;
- 2.2.3.3.1.10. Possuir 02 (duas) fontes de alimentação independentes e redundantes, com tensão de entrada de 120V a 240V AC (manual ou automática), e frequência de 60Hz;
- 2.2.3.3.1.11. Capacidade para suportar Throughput de 5 Gbps de tráfego inspecionado para Firewall, usando-se como base o padrão IMIX (57% de pacotes de 64bytes, 23% de pacotes de 570bytes e 20% de pacotes de 1518bytes); (Amostra)
- 2.2.3.3.1.12. Deve possuir throughput mínimo de 3 (três) GB para tráfego de VPN, considerando-se os padrões criptográficos 3DES e AES;
- 2.2.3.3.1.13. Deve possuir suporte para no mínimo 1.000.000 (um milhão) sessões TCP concorrentes;
- 2.2.3.3.1.14. Cada appliance deve possuir capacidade de suportar no mínimo 80.000 (oitenta mil) novas sessões TCP por segundo;
- 2.2.3.3.1.15. Suportar encaminhamento de pelo menos 1.500.000 (um milhão e quinhentos mil ) pacotes por segundo (pps);
- 2.2.3.3.1.16. Deve suportar a definição de VLAN no firewall conforme padrão IEEE 802.1q e ser possível criar pelo menos 1024 (mil e vinte e quatro) interfaces ou subinterfaces lógicas associadas a VLANs e estabelecer regras de filtragem (Stateful Firewall) entre elas;2.2.3.3.1.10;
- 2.2.3.3.1.17. Possibilitar a utilização de TAG de VLAN até 4096;

#### **2.2.3.3.2. Características do Software de Firewall/Vpn**

- 2.2.3.3.2.1. A licença de uso não faz restrição para o número de usuários que use ou se comunique com o sistema de segurança;
- 2.2.3.3.2.2. Possibilidade de implementação em modo transparente e gateway;

- 2.2.3.3.2.3. Suportar as tecnologias de rede: Ethernet, Fast Ethernet e Gigabit Ethernet;
- 2.2.3.3.2.4. Suportar DHCP relay;
- 2.2.3.3.2.5. Promover a integração com diretórios LDAP para a autenticação de usuários, de modo que o Firewall possa utilizar das informações armazenadas para realizar autenticações;
- 2.2.3.3.2.6. Suportar os esquemas de autenticação de usuários para VPN's, com o uso de token's (exemplo SecureID), RADIUS, senha do sistema operacional, senha do próprio Firewall, diretório LDAP, certificados digitais;
- 2.2.3.3.2.7. Permitir a integração com qualquer Autoridade Certificadora emissora de certificados X.509 que seguir o padrão de PKI (descrito na RFC 2459), inclusive verificando as CRLs (Listas de Certificados Revogados) emitidas periodicamente pelas Autoridades Certificadoras, que devem ser obtidas automaticamente pelo firewall via protocolo HTTP ou LDAP;
- 2.2.3.3.2.8. Suportar controle de aplicações multimídia, tais como voz sobre IP, áudio e vídeo streaming;
- 2.2.3.3.2.9. Realizar NAT estático (1-1) e dinâmico (N-1);
- 2.2.3.3.2.10. Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, Real Áudio, Real Vídeo e RTSP, SIP, H323, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para tráfego outbound (de dentro para fora) quanto inbound (de fora para dentro);
- 2.2.3.3.2.11. Suportar topologias de cluster em alta disponibilidade e/ou em balanceamento de tráfego entre dois ou mais equipamentos de Firewall, de forma que em caso de indisponibilidade de um dos membros, todas as conexões ativas serão direcionadas de forma transparente para o membro ativo;
- 2.2.3.3.2.12. Suportar inspeção stateful de tráfego Ipv6;
- 2.2.3.3.2.13. Deve suportar agrupamento lógico de objetos de configuração ("object grouping") para criação de regras de filtragem. Deve ser possível criar grupos de pelo menos os seguintes tipos de objetos : hosts, redes IP, serviços;
- 2.2.3.3.2.13.1. Deve ser possível verificar a utilização ("hit counts") de cada regra de filtragem ("Access Control Entry") individualmente, independentemente do fato de a configuração da política ter utilizado o conceito de agrupamento lógico de objetos;
- 2.2.3.3.2.14. Suportar SNMP v3;
- 2.2.3.3.2.15. Possuir Mibs SNMP V2/V3 proprietárias, para medir a quantidade de sessões simultâneas de cada túnel VPN;
- 2.2.3.3.2.16. O concentrador VPN deve suportar protocolo Syslog para geração de logs de sistema;
- 2.2.3.3.2.17. Implementar NTP (Network Time Protocol), conforme RFC 1305, contemplando autenticação MD5 entre os peers;
- 2.2.3.3.2.18. Deve ser gerenciável via porta de console, Telnet, SSHv2 e HTTPS;
- 2.2.3.3.2.19. Deve possuir mecanismo interno de captura de pacotes;
- 2.2.3.3.2.20. Deve permitir o armazenamento de pacotes capturados em formato tcpdump;
- 2.2.3.3.2.21. Possibilitar o registro de toda a comunicação realizada através do firewall e de todas as tentativas de abertura de sessões e conexões que por ele forem recusadas;
- 2.2.3.3.2.22. Suportar esquemas de VPN site-to-site em topologias Full Meshed;
- 2.2.3.3.2.23. Suportar, no mínimo, 8.000 (oito mil) conexões VPN IPsec (qualquer combinação entre site-to-site e remote access) simultaneamente; Devem ser fornecidas licenças de clientes IPSEC VPN para pelo menos 8.000 usuários simultâneos; Permitir que o tráfego do cliente remoto de VPN seja direcionado para o site central, para medidas de inspeção do tráfego antes que o mesmo chegue ao seu destino final; Suporte à integração com servidores RADIUS para execução de autenticação, autorização e accounting (AAA) dos usuários que ganharam acesso via conexão VPN ("Extended Authentication");
- 2.2.3.3.2.24. O concentrador VPN deve ser capaz de passar pelo menos os seguintes parâmetros para o cliente: endereço IP do cliente VPN, endereço IP do WINS Server, endereço IP do DNS Server e Default Domain Name;
- 2.2.3.3.2.24.1. A configuração do cliente VPN deve ser completamente automatizada, sendo



exigida do usuário apenas a instalação do cliente VPN em seu PC;

2.2.3.3.2.25. O concentrador de VPN deve ser capaz de configurar nos clientes VPN uma lista de acesso de “split tunneling”, de modo a explicitar quais as redes podem continuar sendo acessíveis de forma direta (sem IPSEC) durante uma conexão VPN à rede corporativa. Deve também ser possível a operação no modo “all tunneling”, em que todo o tráfego do VPN client só poderá ser transportado através da conexão protegida;

2.2.3.3.2.26. O concentrador VPN deve permitir a criação de base de usuários e grupos de usuários que compartilham a mesma política de segurança de forma interna ao equipamento;

2.2.3.3.2.27. O concentrador VPN deve se integrar com servidores RADIUS para que estes façam a atribuição dos endereços IP de VPN (endereços privados) aos clientes;

2.2.3.3.2.28. Suportar pelo menos os seguintes algoritmos de criptografia simétricos: AES256, AES128, DES, e 3DES;

2.2.3.3.2.29. Permitir que os gateways VPN (em uma topologia site-to-site) se autenticuem via pre-shared secret e certificados;

2.2.3.3.2.30. Suportar conexões VPN advindas de clientes L2TP/IPSec nas plataformas Windows 7;

2.2.3.3.2.31. Suportar os algoritmos para geração de chave pública: RSA e Diffie-Hellman, abrangendo os seguintes grupos: Grupo 2 (1024 bits), Grupo 1 (768 bits), Grupo 5 (1536 bits);

2.2.3.3.2.32. Capacidade de aumentar o desempenho de VPN através de soluções de hardware, tais como placas aceleradoras;

2.2.3.3.2.33. Suportar autoridade certificadora integrada ao gateway VPN;

2.2.3.3.2.34. Compatibilidade com certificados digitais (PKI) de terceiros, que cumpram com o padrão X.509 v3;

2.2.3.3.2.35. Deverá suportar certificados digitais padrão ICP-Brasil gerados com chave de 2048 bits e algoritmo de hash SHA2 tanto para autenticação quanto para a assinatura do gateway;

2.2.3.3.2.36. Suportar a integração com autoridades certificadoras de terceiros que possam gerar certificados no formato PKCS#12;

2.2.3.3.2.37. Suportar a solicitação de emissão de certificados à uma autoridade certificadora de confiança (enrollment) via SCEP (Simple Certificate Enrollment Protocol);

2.2.3.3.2.38. Suportar leitura e verificação de Lista de Certificados Revogados através de, no mínimo, HTTP e LDAP;

2.2.3.3.2.39. Suportar NAT-T (NAT Traversal), permitindo a utilização dos clientes VPN em ambientes em que já se efetue PAT (Port Address Translation);

2.2.3.3.2.40. Deve ser possível definir vários templates de conexão no cliente VPN antes que seja enviado para instalação no computador do usuário final. Estes templates devem conter o endereço IP ou nome DNS associado ao concentrador e parâmetros definidores das Security Associations (SAs) a serem usadas nas fases 1 (IKE) e 2 (IPSEC) de negociação dos túneis, incluindo algoritmo de criptografia (DES, 3DES, AES), algoritmo de hash (MD5, SHA), grupo Diffie-Hellman (1, 2, 5 e 7) e tempo de duração (“lifetime”) da conexão;

2.2.3.3.2.40.1. A configuração destes parâmetros deve ser totalmente transparente para o usuário do VPN client;

2.2.3.3.2.41. Deve suportar rotas estáticas com opção para suporte a OSPF e RIPv2;

2.2.3.3.2.42. Além dos túneis IPSEC, a solução deve suportar a terminação de pelo menos 8000 (oito mil) sessões SSL-VPN simultaneamente;

2.2.3.3.2.42.1. Caso esta funcionalidade, seja fornecida através de equipamento adicional, este deverá ser fornecido em appliance que possua fontes redundantes internas e pelo menos 6 interfaces 10/100/1000 autosensing com conector RJ45;

2.2.3.3.2.43. Para SSL VPN devem ser suportadas, no mínimo, as seguintes aplicações transportadas sobre conexões SSL para o concentrador: HTTP, POP3S, IMAP4S, SMTPS;

2.2.3.3.2.44. Para SSL VPN devem ser suportados, via “Port Forwarding”, no mínimo as seguintes aplicações: Telnet, SSH, FTP over SSH, Windows Terminal Services, Outlook/Outlook Express e Lotus Notes;

2.2.3.3.2.45. Deve ser possível criar diferentes grupos de usuários SSL VPN, com definição por grupo, do tipo de serviço permitido sobre as conexões SSL para o concentrador (WEB, e-

mail, sistemas de arquivos);

2.2.3.3.2.46. Deve ser possível especificar as URLs acessíveis através de conexões SSL VPN;

2.2.3.3.2.47. Deve ser possível a criação de portal personalizado ("portal customization") para acesso SSLVPN. O portal deve refletir os recursos disponíveis (aplicações e URLs acessíveis, possibilidade de download do cliente SSL VPN, "banner de acesso") para o grupo a que o usuário que requisita acesso pertence;

2.2.3.3.2.48. Deve ser possível definir no concentrador VPN o mapeamento de atributos LDAP, Active Directory e RADIUS para parâmetros existentes na configuração local de grupos do concentrador. Deve ser possível escolher, para cada grupo, se os parâmetros usados serão os definidos localmente ou os mapeados de um grupo externo LDAP/RADIUS;

### **2.2.3.3.3. Características do software de gerenciamento e administração**

2.2.3.3.3.1. Permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras em todos os clusters;

2.2.3.3.3.2. Suportar o gerenciamento de objetos de rede para utilização em regras de acesso. Deve ser possível criar, no mínimo, os seguintes tipos de objetos: hosts, gateways, firewalls, clusters, redes, faixas de endereços, NAT, usuários, VPNs. Deverá ainda permitir detectar se e onde, na base de regras, está sendo utilizado determinado objeto de rede.

(AMOSTRA)

2.2.3.3.3.3. O licenciamento e o software não devem limitar o número de objetos, regras de segurança, NAT, endereços IP e usuários de VPN SSL;

2.2.3.3.3.4. Suportar agrupamento lógico de objetos ("object grouping") para criação de regras de filtragem;

2.2.3.3.3.5. Possibilitar a especificação de política por tempo, ou seja, permitir a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

(AMOSTRA)

2.2.3.3.3.6. Implementar a contabilização das Regras de Controle de Acesso por ela gerenciadas;

2.2.3.3.3.7. A solução deve permitir o agrupamento lógico de dispositivos físicos, de acordo com a funcionalidade e com a localização física dos mesmos, permitindo o gerenciamento simultâneo de vários elementos;

2.2.3.3.3.8. Permitir a reutilização de objetos lógicos em várias políticas de Segurança;

(AMOSTRA)

2.2.3.3.3.9. Permitir o retorno emergencial às configurações anteriores dos dispositivos, para a necessidade de recuperação de falhas ("Rollback de configuração");

2.2.3.3.3.10. Permitir distribuição centralizada de pacotes de atualização;

2.2.3.3.3.11. A solução deve ser capaz de testar a conectividade dos equipamentos gerenciados;

2.2.3.3.3.12. Suportar configuração das funcionalidades de alta disponibilidade dos dispositivos físicos;

2.2.3.3.3.13. Permitir a visualização de qual parte da topologia gerenciada (origem, destino, serviço) está sendo afetada por determinada regra;

2.2.3.3.3.14. Permitir a detecção de alteração e tentativas de alteração da configuração dos dispositivos físicos;

2.2.3.3.3.15. Prover funcionalidade para análise e auditoria de regras com capacidade de detectar regras conflitantes, regras equivalentes ou um conjunto;

2.2.3.3.3.16. Suportar operação em modo de "workflow", ou seja, permitir que as regras sejam aplicadas somente após passar por um fluxo de aprovação gerencial;

2.2.3.3.3.17. Suportar acesso baseado em perfil de usuário com as permissões de visualizar, modificar, aprovar e distribuir por tipo de objeto e política;

2.2.3.3.3.18. Deve ser possível definir os perfis de acesso à solução ("Role Based Access Control" = RBAC) no sistema de Gerência de Controle de Acesso fornecido;

2.2.3.3.3.19. Suportar a configuração de VPN dos tipos "site-to-site" e "client-to-site";

Permitir a identificação e exclusão de regras e objetos que estão aplicadas nos dispositivos,

mas não afetam o desempenho e a segurança da rede (regras e objetos em desuso sob o ponto de vista lógico);

2.2.3.3.3.20. A solução, de Cluster de Firewall e Gerência, deve suportar protocolo de autenticação para controle do acesso administrativo ao equipamento que possua pelo menos as seguintes características:

2.2.3.3.3.20.1. Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega;

2.2.3.3.3.20.2. Criptografar todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;

2.2.3.3.3.20.3. Registrar todos os comandos executados por um dado usuário na execução de comandos (accounting);

2.2.3.3.3.20.4. Permitir atribuição de perfis incluindo: usuário (somente leitura), administradores e monitores com níveis de permissão diferenciados;

2.2.3.3.3.20.5. Possibilitar o gerenciamento (incluindo a criação, alteração, monitoração e exclusão) de objetos de rede. Os tipos de objetos deverão permitir especificar de forma distinta recursos tais como: Hosts, Gateways, Firewalls, Clusters (alta-disponibilidade), Redes, Faixas de endereços, NAT, Usuários, Agrupamento de objetos e VPNs;

2.2.3.3.3.20.6. Os softwares utilizados para acessar as gerências e realizar tarefas administrativas (GUI clients) deverão ser compatíveis com o sistema operacional Linux.

2.2.3.3.3.20.6.1. Caso não haja tal compatibilidade, deverão ser fornecidas 3 (três) licenças para o sistema operacional proprietário disponibilizado.

## 2.8. Das Quantidades

ITEM	DESCRIÇÃO	QUANTIDADE			TOTAL
		REGISTRO	1ª AQUISIÇÃO	RESERVA	
I	Cluster de Firewall - Porj RFB - BSA e SPO		02 clusters		
II-I	Cluster Firewall/VSX - Configuração I		01 cluster		
II-II	Cluster Firewall/VSX - Configuração II		01 cluster		
III-I	Ambiente Interno - Configuração I		45		
III-II	Ambiente Interno - Configuração II		6		
III-III	Ambiente Interno - Configuração III		6		

## 2.9. Da Entrega e do Prazo de Entrega

2.9.1. Entende-se por cumprimento do prazo de entrega o recebimento dos componentes de cada solução especificada, sua instalação e execução dos serviços no SERPRO, deixando-os operacionais para o aceite definitivo. O não cumprimento rigoroso do prazo de entrega, ou entrega parcial, ou entrega de configuração inferior a solicitada implicará em rescisão do contrato a ser firmado entre o SERPRO e a CONTRATADA.

2.9.2. Cada solução com seus componentes adquiridos no edital, bem como os softwares básicos, os serviços de instalação e migração de ambientes, capacitações e os serviços de implementação do ambiente de contingência deverão ser entregues, instalados e estar operacionais, conforme definido abaixo:

2.9.2.1. Cada solução com seus componentes deverá ser entregue instalada e configurada conforme solicitado no edital, de forma a estarem operacionais em até 90 (noventa) dias corridos a partir da assinatura do contrato.

2.9.2.1.1. Para entrega dos produtos, que compõem cada solução, a CONTRATADA terá um prazo de 60 (sessenta) dias corridos para entrega, nas localidades a serem definidas pelo

SERPRO, no ato de assinatura do contrato, onde receberão aceite provisório para liberação da 1ª parcela de pagamento.

## 2.10. Localidades de Entrega, de Instalação e Manutenção

<b>REGIONAL BRASÍLIA/DF</b> ENDEREÇO: SGAN AV. L2 Norte, Quadra 601 Módulo "G" CEP: 70836-900 TELEFONE: (61) 2021.9000 FAX: (61) 2021.9691 INSCRIÇÃO ESTADUAL: 07334743/002-94 INSCRIÇÃO MUNICIPAL : 07334743/002-94 CNPJ: 33.683.111/0002-80	<b>REGIONAL RIO DE JANEIRO – HORTO</b> ENDEREÇO: Rua Pacheco Leão, no 1.235, Fundos Jardim Botânico CEP: 22460-030 TELEFONE: (21)2559.3300 FAX: (21) 2117.4178 INSCRIÇÃO ESTADUAL: ISENTO INSCRIÇÃO MUNICIPAL: 00940895 CNPJ: 33.683.111/0008-75
<b>REGIONAL BELÉM/PA</b> ENDEREÇO: Av. Perimetral da Ciência, no 2010, Terra Firme CEP: 66077-530 TELEFONE: (91) 4008 1777 FAX: (91) 4008 1800 INSCRIÇÃO ESTADUAL: ISENTO INSCRIÇÃO MUNICIPAL: 025.983-8 CNPJ: 33.683.111/0003-60	<b>REGIONAL RIO DE JANEIRO – ANDARAÍ</b> ENDEREÇO: Rua Duquesa de Bragança nº 100 Grajaú CEP: 22460-905 TELEFONE: (21)2459.3300 FAX: (21) 2117.4178 INSCRIÇÃO ESTADUAL: 10.004.799 (Facultativa) INSCRIÇÃO MUNICIPAL: (Aguardando Liberação) CNPJ: 33.683.111/0018-47
<b>REGIONAL FORTALEZA/CE</b> ENDEREÇO: Av. Pontes Vieira, no 832 São João do Tauapé CEP: 60130-240 TELEFONE: (85) 4008 2800 FAX: (85) 4008 2902 INSCRIÇÃO ESTADUAL: ISENTO INSCRIÇÃO MUNICIPAL: 016155-1 CNPJ: 33.683.111/0004-41	<b>REGIONAL SÃO PAULO/SP</b> ENDEREÇO: Rua Olívia Guedes Penteado, no 941 Capela do Socorro CEP: 04766-900 TELEFONE: (11) 2173 1322 FAX: (11) 2173 1739 INSCRIÇÃO ESTADUAL: 111.445.700.110 INSCRIÇÃO MUNICIPAL: 8242433-0 CNPJ: 33.683.111/0009-56
<b>REGIONAL RECIFE/PE</b> ENDEREÇO: Av. Parnamirim, no 295 Parnamirim CEP: 52060-000 TELEFONE: (81) 2126 4000/4011 FAX: (81) 2126 4028 INSCRIÇÃO ESTADUAL: ISENTO INSCRIÇÃO MUNICIPAL: 006.632.0 CNPJ: 33.683.111/0005-22	<b>ESCRITÓRIO SÃO PAULO/SP</b> ENDEREÇO: Rua Plínio Ramos, 99 Bairro da Luz CEP: 01027-010 TELEFONE: (11) 2173.1101 / 1732 FAX: (11) 2173.1972 INSCRIÇÃO ESTADUAL: ISENTO INSCRIÇÃO MUNICIPAL: 3.251.788-2 CNPJ: 33.683.111/0016-85
<b>REGIONAL SALVADOR/BA</b> ENDEREÇO: Av. Luiz Viana Filho, No 2355 Bairro Paralela CEP: 41130-530 TELEFONE: (71) 2102 7800 FAX: (71) 2102 7855 INSCRIÇÃO ESTADUAL: ISENTO INSCRIÇÃO MUNICIPAL: 000.555/001-77 CNPJ: 33.683.111/0006-03	<b>REGIONAL CURITIBA/PR</b> ENDEREÇO: Rua Carlos Pioli, n.o 133 Bairro Bom Retiro CEP: 80520-170 TELEFONE: (41) 3313.8200 FAX: (41) 3313.8346 INSCRIÇÃO ESTADUAL: ISENTO INSCRIÇÃO MUNICIPAL: 105.663-1 CNPJ: 33.683.111/0010-90

<b>REGIONAL BELO HORIZONTE/MG</b> ENDEREÇO: Av. José Cândido da Silveira, no 1.200 Cidade Nova CEP: 31170-000 TELEFONE: (31) 3311 6200 FAX: (31) 3311 6320 INSCRIÇÃO ESTADUAL: ISENTO INSCRIÇÃO MUNICIPAL: 305698/001-3 CNPJ: 33.683.111/0007-94	<b>ESCRITÓRIO DE FLORIANÓPOLIS/SC</b> ENDEREÇO: Rodovia José Carlos Daux (SC 401), no 600 Edifício Alfama, 2o andar, Parque Tecnológico Alfa, Bairro João Paulo. CEP: 88040-901 TELEFONE: (48) 3231 8800 FAX: (48) 3231 8888 INSCRIÇÃO ESTADUAL: ISENTO INSCRIÇÃO MUNICIPAL: 20278-9 CNPJ: 33.683.111/0019-28
	<b>REGIONAL PORTO ALEGRE/RS</b> ENDEREÇO: Av. Augusto de Carvalho, no 1.133 Cidade Baixa CEP: 90010-390 TELEFONE 21291200 FAX: (51) 2129 1399 INSCRIÇÃO ESTADUAL: ISENTO INSCRIÇÃO MUNICIPAL: 0241622-0 CNPJ: 33.683.111/0011-70

### 3.0 Níveis de Serviço

#### 3.1. Suporte técnico à Solução ofertada

3.1.1. Possuir suporte técnico para a solução, bem como para seus acessórios, durante o período de vigência do contrato, assegurando prazos, de atendimento, compatíveis com a instalação, ou seja, 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana (à exceção dos chamados de Severidade 4), para um período de 48 (quarenta e oito) meses.

3.1.2. O atendimento aos chamados deverá obedecer à seguinte classificação quanto ao nível de severidade:

Severidade	Descrição	Tipo de Atendimento	Tempo de Atendimento	Tempo de Solução
1	Crítica	On-site	No máximo 2 (duas) horas após a abertura do chamado, incluindo percurso do técnico até as instalações do SERPRO.	No máximo 4 (quatro) horas após o início do atendimento do chamado.
2	Alta	On-site	No máximo 2 (duas) horas após a abertura do chamado, incluindo percurso do técnico até as instalações do SERPRO.	No máximo 8 (oito) horas após o início do atendimento do chamado.
3	Média	Remoto, com exceção das situações em que seja necessária intervenção física.	No máximo 4 (quatro) horas após a abertura do chamado.	No máximo 10 (dez) horas após o início do atendimento do chamado.
4	Baixa	Remoto	No máximo 24 (vinte e quatro) horas após a abertura do chamado.	No máximo 72 (setenta e duas) horas após a abertura do chamado.

#### 3.2. Chamados, Registros e Início de Prazos

3.2.1. Será aberto um chamado para cada problema reportado.

3.2.2. A abertura do chamado na CONTRATADA pelo SERPRO poderá ser realizado através de telefone ou WEB.

3.2.3. Os prazos para atendimento de chamados de qualquer severidade serão considerados a partir da hora em que o chamado é aberto, isto é, registrado na CONTRATADA, recebendo dela uma identificação para acompanhamento, controle e histórico.

3.2.4. Será aberto um chamado técnico para cada problema reportado, sendo iniciada a

contagem do tempo de atendimento a partir da hora de acionamento.

### **3.2.5. Tratamento dos chamados de Severidade 1**

3.2.5.1. Os chamados de Severidade 1 serão atendidos on-site em no máximo 2 (duas) horas após a sua abertura, incluindo o percurso do técnico até as instalações do SERPRO e contarão com esforço concentrado da contratada com vistas a aplicar solução ou medida de contorno em até 4 (quatro) horas após o início do atendimento do chamado.

3.2.5.2. O atendimento de Severidade 1 não poderá ser interrompido até o completo restabelecimento do produto envolvido, mesmo que se estenda por períodos noturnos e dias não úteis.

3.2.5.3. O atendimento de Severidade 1 somente será efetuado pelo fabricante da Solução ou do item da Solução (no caso de composição de produtos para empacotamento da Solução), mesmo que se estenda por períodos noturnos e dias não úteis.

3.2.5.3.1. No caso de composição da Solução entre vários fabricantes todos deverão ser acionados pela CONTRATADA, para conclusividade da ocorrência.

### **3.2.6. Tratamento dos chamados de Severidade 2**

3.2.6.1. Os chamados de Severidade 2 serão atendidos on-site em no máximo 2 (duas) horas após a sua abertura, incluindo o percurso do técnico até as instalações do SERPRO e contarão com esforço concentrado da contratada com vistas a aplicar solução ou medida de contorno em até 8 (oito) horas após o início do atendimento do chamado.

3.2.6.2. O atendimento de Severidade 2 não poderá ser interrompido até o completo restabelecimento do produto envolvido, mesmo que se estenda por períodos noturnos e dias não úteis.

3.2.6.3. Os chamados classificados com Severidade 2, quando não solucionados no tempo definido, serão automaticamente escalados para Severidade 1, sendo que os prazos de atendimento e de solução serão automaticamente escalados para o novo nível de severidade.

### **3.2.7. Tratamento dos chamados de Severidade 3**

3.2.7.1. Os chamados de Severidade 3 serão atendidos em no máximo 4 (quatro) horas após a sua abertura e contarão com esforço concentrado da contratada com vistas a aplicar solução ou medida de contorno em até 10 (dez) horas após o início do atendimento do chamado.

3.2.7.2. Caso o problema não possa ser resolvido remotamente, a contratada deverá colocar à disposição do SERPRO, um especialista devidamente habilitado e credenciado que trabalhará o tempo que for necessário para a solução do problema, sendo que o ônus financeiro de tal providência será da contratada.

3.2.7.3. Os chamados classificados com Severidade 3, quando não solucionados no tempo definido, serão automaticamente escalados para Severidade 2, sendo que os prazos de atendimento e de solução serão automaticamente escalados para o novo nível de severidade.

### **3.2.8. Tratamento dos chamados de Severidade 4**

3.2.8.1. Os chamados de Severidade 4 serão atendidos em no máximo 24 (vinte e quatro) horas após a sua abertura e deverão ser concluídos em até 72 (setenta e duas) horas após a abertura do chamado.

3.2.8.2. Os chamados classificados com Severidade 4 serão atendidos em horário comercial, ou seja, das 08h00min às 18h00min, de segunda-feira a sexta-feira, horário de Brasília.

3.2.9. Por necessidade de serviço, o SERPRO poderá solicitar a escalação de chamado para níveis superiores de severidade. Os prazos dos chamados escalados passam a contar novamente do início.

### **3.2.10. Manutenções**

3.2.10.1. A CONTRATADA deverá prover, sempre que necessário, todas as correções e atualizações dos hardwares instalados, tais como: nível de firmware e microcódigos, que

permitam melhorar as funcionalidades dos equipamentos, bem como mantê-los compatíveis com os demais componentes de hardware e software dos Centros de Dados do SERPRO, sem ônus adicional para o SERPRO.

3.2.10.2. A CONTRATADA deverá realizar manutenção preventiva de acordo com o especificado no Manual do Fabricante do equipamento, tanto do hardware quanto do firmware instalados, sendo de responsabilidade do fornecedor prover todas as correções e atualizações necessárias, de forma sistemática e programada.

3.2.10.3. No caso de manutenções, preventivas ou corretivas, em que haja risco de indisponibilidade total ou parcial dos equipamentos, o SERPRO deverá ser previamente notificado para que se proceda à aprovação e o agendamento da manutenção em horário conveniente ao SERPRO.

3.2.10.4. Em qualquer hipótese (e ainda que não seja o fabricante dos equipamentos) a CONTRATADA deverá possuir acesso para suporte técnico de 2º e 3º níveis, bem como aos firmwares e microcódigos dos equipamentos, de forma a prestar os serviços de manutenção e assistência técnica, sem ônus adicional para o SERPRO. Para todos os efeitos da contratação em espécie, vigoram os seguintes conceitos:

3.2.10.5. Suporte Técnico Primeiro Nível: equipe treinada para atender diretamente os usuários em demandas referentes a diagnóstico e tratamento de problemas, configuração e administração do ambiente e esclarecimento de dúvidas em geral.

3.2.10.6. Suporte Técnico Segundo Nível: equipe multidisciplinar treinada, certificada e com grande experiência em ambientes críticos e complexos, que exigem alta disponibilidade.

3.2.10.7. Suporte Técnico Terceiro Nível: escalonamento obrigatório ao fabricante, devido à necessidade de retaguarda nas tecnologias suportadas.

### **3.2.11. Canais de atendimento**

3.2.11.1. Atendimento através de canal telefônico gratuito 0800, 24 (vinte e quatro) horas por dia, 7(sete) dias por semana.

3.2.11.2. Chamado técnico através de site na Internet, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana ou canal telefônico gratuito 0800.

### **3.2.12. Escalação de Severidade**

3.2.12.1. Por necessidade de serviço ou criticidade do problema, o SERPRO poderá solicitar a escalação de chamado para níveis superiores ou inferiores de severidade ou seus respectivos prazos.

### **3.2.13. Monitoramento do Atendimento dos Chamados**

3.2.13.1. Todos os chamados serão controlados por sistema de informação da CONTRATADA.

3.2.13.2. Para efeito de acompanhamento das providências e do tempo decorrido desde a sua abertura, o SERPRO será informado sobre cada abertura e fechamento de chamado efetuado por força da presente contratação.

3.2.13.3. O fechamento do chamado poderá se dar quer pela aplicação de correção ao produto ou pela aplicação de solução de contorno que possibilite a operação do sistema.

3.2.13.4. A disponibilização de medida corretiva definitiva poderá, a critério da CONTRATADA, vir a ser incorporada em futuras versões do software.

3.2.13.5. Antes do fechamento de cada chamado a CONTRATADA consultará o SERPRO para validar o fechamento do chamado.

3.2.13.6. Um chamado fechado sem anuência do SERPRO ou sem que o problema tenha sido de fato resolvido, será reaberto e os prazos serão contados a partir da abertura original do chamado, inclusive para efeito de aplicação das sanções previstas.

3.2.13.7. A CONTRATADA manterá cadastro das pessoas indicadas pelo SERPRO que poderão efetuar abertura e autorizar fechamento de chamados.

### **3.2.14. Relatórios sobre a Prestação dos Serviços**

3.2.14.1. A CONTRATADA emitirá relatórios mensais referentes à prestação dos serviços,

incluindo informações sintéticas dos chamados abertos e fechados, com ênfase para aqueles resolvidos no mês, informações sobre a disponibilização de novas versões e outras informações consideradas de relevância.

3.2.14.2. A CONTRATADA deve incluir nos relatórios no mínimo as informações do técnico do SERPRO responsável pela abertura do chamado, nível de severidade do chamado, a data e hora da abertura, data e hora do fechamento e solução aplicada.

### **3.3. Penalidades**

3.3.1. A interrupção do atendimento de um chamado por parte da CONTRATADA, que não tenha sido previamente autorizada pelo SERPRO, ensejará aplicação de multa, conforme o nível de severidade do mesmo:

3.3.2. O não atendimento dentro do prazo estabelecido para o chamado ensejará aplicação de multa à contratada, conforme o nível de severidade do mesmo:

Severidade 1 – 0,13% (treze décimos por cento) do valor TOTAL da aquisição constante no contrato para o item (equipamento) correspondente, por hora ou fração de hora de atraso.

Severidade 2 – 0,10% (dez décimos por cento) do valor TOTAL da aquisição constante no contrato para o item (equipamento) correspondente, por hora ou fração de hora de atraso.

Severidade 3 – 0,05% (cinco centésimos por cento) do valor TOTAL da aquisição constante no contrato para o item (equipamento) correspondente, por hora ou fração de hora de atraso.

Severidade 4 – 0,03% (três centésimos por cento) do valor TOTAL da aquisição constante no contrato para o item (equipamento) correspondente, por hora ou fração de hora de atraso.

## **4.0 Estimativa de Valor**

### **4.2. Forma de Pagamento**

4.2.1. O pagamento à Contratada será efetuado no primeiro dia útil após o 20º (vigésimo) dia corrido da data do recebimento da nota fiscal e/ou fatura. Para a liberação do pagamento ocorrerá conforme descrito abaixo e somente ocorrerá após o recebimento dos produtos e a emissão do aceite definitivo de cada etapa, pelo Responsável Técnico Operacional e CORAC Regional, nas localidades definidas pelo Serpro, no ato da assinatura do contrato.

4.2.2. Primeira Parcela: 50% (cinquenta por cento) do valor do item da Solução (hardware e software), descritos no contrato, paga após a emissão do termo de aceite definitivo da 1ª Etapa (entrega do item da Solução);

4.2.3. Segunda Parcela: 50% (cinquenta por cento) do valor total de aquisição, descritos no contrato, paga somente após o aceite definitivo da aquisição, pelas áreas envolvidas;

4.3. Todas as Notas Fiscais deverão conter suas respectivas alíquotas de imposto;

4.3.1. Nos preços mencionados estão inclusas todas as despesas, tais como: taxas, impostos, frete, seguro, embalagens, manuais, despesas de transporte e garantia de funcionamento e atualização de versão dos programas, suporte técnico, repasse de conhecimento durante o período de 60 (sessenta) meses.

4.4. As Notas Fiscais e/ou Faturas deverão ser entregues em duas vias no protocolo geral do Serpro nas Regionais definidas pelo Serpro, para instalação da Solução;

4.5. Constatando-se alguma incorreção na Nota Fiscal e/ou Fatura, o prazo para pagamento será contado a partir da respectiva regularização. Carta de Correção só será admitida para regularizar os dados cadastrais do Serpro. Deverá constar no corpo da nota fiscal e/ou fatura, o número do Contrato e do respectivo processo, além do banco, agência e número da conta onde deverá ser feito o pagamento;

4.6. A Razão Social do Serpro na nota fiscal e/ou fatura deverá ser: SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS (SERPRO);

4.7. A Contratada deverá informar o CNPJ que será utilizado na emissão das notas fiscais e/ou faturas e e-mail.



## **5.0 Justificativa**

### **6.0 Seleção do Contratado**

O certame licitatório será através de Pregão Eletrônico, com criação de ata de registro de Preços para uso exclusivo do Serpro, inicialmente pelo menor preço ofertado e a seleção da contratada dar-se-á nas seguintes condições:

#### **6.1. Documentação e Homologação**

6.1.1. A LICITANTE com a proposta de menor preço deverá apresentar em até 05 (cinco) dias úteis após solicitação do pregoeiro, documentação técnica do fabricante da solução comprovando o atendimento a todos os requisitos contidos na Especificação do objeto a ser contratado, bem como o atendimento das seguintes condições:

6.1.1.1. Documentação técnica do fabricante. Nessa documentação, a LICITANTE deve fornecer uma planilha ponto-a-ponto indicando documento e página onde consta o cumprimento de cada um dos requisitos das especificações técnicas;

6.1.1.2. Não serão aceitas referências a futuros releases ou versões de produtos para comprovar a existência ou aderência à qualquer quesito desta especificação;

6.1.1.3. Cada documento apresentado deve descrever claramente a referência ao modelo apresentado na proposta, não sendo válidas referências genéricas, e deverão seguir as formas de apresentação definidas na Especificação do Objeto;

6.1.1.4. Será aceita Carta do Fabricante, como comprovação de atendimento de requisitos técnicos e de compatibilidade especificados neste edital, apenas para os itens que não constarem na documentação da maioria dos fabricantes ou que não puderem ser mensurados;

6.1.1.5. Não será aceita Carta do Fornecedor, como comprovação de atendimento a requisitos técnicos e de compatibilidade especificados neste edital;

6.1.1.6. Relação de componentes, incluindo módulos, fontes e acessórios, de cada equipamento que compõe a solução, contendo o código do produto (fabricante) e as respectivas quantidades em cada item;

6.1.1.7. Caso, a documentação apresentada deixe de comprovar o atendimento de um único item da especificação técnica, a proposta será desclassificada, exceto no caso da apresentação de Carta do Fabricante, não passando para a etapa seguinte de testes das funcionalidades especificadas;

6.1.1.8. A proposta comercial a ser apresentada pela LICITANTE deverá discriminar os valores de todos os itens que compõem a solução ofertada, incluindo hardware, software e acessórios;

6.1.1.9. Avaliação prática, das EMPRESAS LICITANTES CLASSIFICADAS E APTAS, em bancada de testes de características e funcionalidades exigidas nos itens: ITEM I, ITEM II e ITEM III, separadamente especificado;

6.1.1.9.1. Esta etapa caberá às EMPRESAS LICITANTES CLASSIFICADAS E APTAS, para todos os subitens especificados, comprovar na prática, através de testes de bancada, as características e funcionalidades exigidas, onde deverão ser utilizados equipamentos de homologação de cada EMPRESA LICITANTE CLASSIFICADA E APTA – não incorrendo em encargos ao SERPRO;

6.1.1.9.2. Esta etapa será executada por prepostos do SERPRO em conjunto com os prepostos da EMPRESAS LICITANTES CLASSIFICADAS E APTAS no item específico da aquisição.

6.1.1.9.3. Cada ITEM será homologado em fase sequencial, conforme cronograma que será disponibilizado pelo Serpro;

6.1.1.9.4. Somente será efetuado a fase de homologação do próximo item da presente aquisição, quando o item anterior estiver devidamente homologado;

6.2. Toda homologação deverá ser realizada nas dependências do SERPRO de Brasília;

6.3. Somente após a etapa de homologação será definida a EMPRESA LICITANTE VENCEDORA do processo licitatório no referido item;

6.3.1. Todos os testes e relacionamento dos técnicos da LICITANTE com o SERPRO deverão ser efetuados no idioma português;

6.3.1.1. Ao fim de cada dia de testes, deverá ser emitida e distribuída Ata de Atividades e Ocorrências a todos os presentes;

6.3.2. Caso apenas um subitem referente às especificações seja considerado não atendido, a proposta será totalmente desclassificada;

6.3.3. Para cada ITEM a LICITANTE deverá indicar previamente os nomes de, no máximo, 06 (seis) técnicos para participação integral durante a realização dos testes de bancada e homologação. Esses técnicos deverão ser representantes legais da LICITANTE, comprovado através documentação de vínculo contratual ou procuração;

6.3.4. Para cada ITEM a LICITANTE deverá indicar previamente os nomes dos seus técnicos responsáveis pela instalação dos equipamentos nas dependências do SERPRO em número a ser definido pela proponente;

6.3.5. A critério de cada LICITANTE, as etapas do aceite poderão ser acompanhados por técnico do fabricante;

6.3.6. Dos técnicos indicados pela LICITANTE, vencedora do respectivo ITEM, apenas um poderá ser substituído após o início dos testes de bancada, desde que seja comunicado formalmente ao SERPRO;

6.3.7. As empresas concorrentes do pregão poderão indicar técnicos (apenas um para cada empresa) para acompanhar os testes de bancada. As indicações deverão ser realizadas com, no mínimo, 2 (dois) dias de antecedência e apenas serão permitidos questionamentos diretos aos técnicos do SERPRO;

6.3.8. No caso de ausência, em qualquer dos períodos durante a realização dos testes de bancada, dos técnicos indicados pelas demais empresas concorrentes do pregão, não serão aceitos quaisquer questionamentos sobre sua realização;

6.3.9. Durante a realização dos testes de bancada serão permitidas somente 02 (duas) atualizações de software e sistema operacional dos equipamentos sob avaliação, visando a correção ou adaptação para atendimento aos requisitos do edital. Essas atualizações poderão corrigir mais de um item simultaneamente;

6.3.9.1 A critério do Serpro os testes de bancada poderão ser reiniciados após atualização de versão.

6.3.10. Os testes deverão ser realizados no horário compreendido entre 09:00 h e 17:00 h de segunda a sexta-feira;

6.3.11. A modalidade para realização da aquisição será pregão eletrônico e a adjudicação será pelo menor valor global.

#### **6.4. Homologação da Solução**

6.4.1. Após aceite da documentação comprobatória, a LICITANTE deverá disponibilizar para a realização das etapas de homologação, no prazo de até 10 (dez) dias corridos contados à partir da solicitação do pregoeiro, amostra da mesma marca e modelo ofertado na proposta, conforme especificação do objeto;

6.4.2. Cada LICITANTE homologado deverá disponibilizar adicionalmente todos os demais equipamentos necessários para a realização dos testes de bancada;

6.4.3. O SERPRO fornecerá um prazo de 10 (dez) dias úteis para a realização da fase de homologação;

6.4.4. O prazo de homologação poderá ser prorrogado por igual período a critério do SERPRO.

### **7.0 Justificativa para Aceitação de Preços**

## **8.0 Gerenciamento do Contrato**

### **Obrigações do SERPRO**

8.1. Faculta-se o SERPRO e a CONTRATADA, sempre quando necessário, agendar reuniões periódicas de caráter gerencial ou técnico para avaliar os trabalhos, adotar resoluções e obter esclarecimento de pendências durante toda a vigência do contrato e garantia;

8.2. O SERPRO se reserva no direito de remanejar a solução contratada entre suas Regionais e Escritórios, no Território Nacional;

### **Obrigações da CONTRATADA**

8.3. Repasse de Conhecimento (para cada ITEM da Especificação Técnica);

8.3.1. Como parte integrante do processo de instalação, configuração, implantação, implementação e produção, a empresa vencedora deverá realizar o repasse de conhecimento para o SERPRO, dos conhecimentos necessários para instalar, administrar, configurar, operar, desenvolver e gerenciar os produtos fornecidos, conforme descrito a seguir:

8.3.1.1. As capacitações tecnológicas terão conteúdo e carga horária em consonância com os cursos oficiais do fabricante da solução, vigentes à época da sua realização.

8.3.1.2. O repasse de conhecimento para o SERPRO deverá ser iniciado em até 30 (trinta) dias após o aceite da solução, podendo ser adiada por conveniência do SERPRO, quando então, em comum acordo com a CONTRATADA, será marcada a data definitiva;

8.3.1.3. A licitante vencedora deverá entregar o conteúdo programático (ementa) de todos os treinamentos, para aprovação pelo SERPRO;

8.3.1.4. Após a assinatura do contrato, a empresa vencedora deverá fornecer o repasse de conhecimento, através de repasse de conhecimento, para o SERPRO em 03 (três) localidades a serem definidas pelo SERPRO, para até 12 (doze) pessoas por localidade, abrangendo: administração, configuração básica e avançada, gerenciamento, desenvolvimento e novas funcionalidades. O conteúdo poderá ser redefinido de acordo com as necessidades do SERPRO;

8.3.1.5. A data de início destas capacitações adicionais e o local de realização serão definidos pelo SERPRO de acordo com suas necessidades. O SERPRO deverá comunicar formalmente o fornecedor com uma antecedência mínima de 60 (sessenta) dias;

8.3.1.6. O repasse de conhecimento deverá possuir carga horária mínima de 40 (quarenta) horas e deverá ocorrer em período integral;

8.3.1.7. O repasse de conhecimento deverá ser ministrada por profissional(ais) certificado(s) ou autorizado(s) pelo fabricante da(s) solução(ões);

8.3.1.7.1. O conteúdo deve ser oficial e reconhecido pelo fabricante;

8.3.1.8. A contratada deverá apresentar com antecedência de, no mínimo, 10 (dez) dias do início do repasse de conhecimento, os certificado(s) solicitado(s) bem como declaração de que a empresa está autorizada pelo fabricante a prestar a capacitação;

8.3.1.9. O material do repasse de conhecimento deve ser original e de boa qualidade e aprovado pelo SERPRO;

8.3.1.10. Todas as despesas com material, equipamentos, instrutores, deslocamento de instrutores e demais itens serão de responsabilidade do fornecedor;

8.3.1.11. Após cada repasse de conhecimento deverá ser emitido certificado para cada participante, obedecendo aos critérios de frequência previamente negociados com o SERPRO;

8.3.2. O não atendimento a um dos itens e subitens descritos em repasse de conhecimento para o SERPRO ensejará aplicação de multa à CONTRATADA no valor equivalente a 1,0% (um por cento) do valor do contrato, por hora ou fração de hora de atraso, limitado a 20% (vinte por cento) do valor total do contrato;

8.3.3. Os custos de deslocamento dos profissionais do SERPRO selecionados para o repasse de conhecimento para o SERPRO, quando existirem, será de responsabilidade do SERPRO;

8.3.4. A CONTRATADA deverá prover toda a logística e todo o material necessário à execução do repasse de conhecimento teórico e prático, ou seja, instalações adequadas, equipamentos, manuais e apostilas didáticas. Os manuais e apostilas fornecidos devem ser

originais e oficiais do fabricante;

8.3.5. O repasse de conhecimento deverá ser realizado utilizando conteúdo teórico e prático, através de laboratório preparado com equipamentos equivalentes aos ofertados, onde estarão disponíveis as mesmas funcionalidades solicitadas nas especificações técnicas dos itens;

8.3.6. A cada ano ou cada grande atualização de versão, considerada pelo Serpro, a empresa contratada deverá ser realizar workshop, tendo como base o Perfil de Administrador, onde após esses eventos os empregados deverão estar aptos a Administrar, Configurar, Operar e Gerenciar a solução contratada;

8.3.7. Para atendimento ao item 8.3.6 o Serpro definirá com a CONTRATADA a melhor forma de implementação desses eventos;

8.3.8. Toda documentação referente a manual de usuário deverá ser completa e em inglês ou português;

8.3.9. Os contratos serão gerenciados por um Gestor Técnico da área de operações e pela área de gestão de contratos.

## **9.0 Considerações Gerais**

9.1. O prazo de vigência do contrato será de 12 (doze) meses, contado a partir da data de assinatura;

9.2. O prazo de garantia dos produtos ofertados para cada item da especificação técnica será de 48 (quarenta e oito) meses;

9.3. A empresa Licitante deverá apresentar documento(s) que comprove(m) a aptidão técnica necessária para executar o objeto, tais como contrato, termo, certificado, declaração, endereço eletrônico de sítios oficiais do fabricante na internet, entre outros documentos pertinentes que demonstrem de forma inequívoca, a habilidade técnica para prestar o serviço de suporte técnico e vínculo vigente com o fabricante do hardware e do software;

9.4. Não haverá necessidade de apresentação da declaração prevista no item 9.3, quando a licitante for a própria fabricante do hardware e software;

9.5. O objeto da presente contratação está caracterizado como bens ou serviços de informática ou automação, conforme definição constante no Art. 16-A da Lei nº 8.248, de 23 de outubro de 1991;

9.6. Os serviços especificados possuem características de serviços contínuos, sem dedicação exclusiva de mão de obra;

9.7. A Ata de Registros de Preços a ser criada será de uso exclusivo do Serpro em toda sua capilaridade geográfica descrita no item 2.10 da Especificação Técnica.