



SENADO FEDERAL

Secretaria de Administração de Contratações – SADCON
 Coordenação de Planejamento e Controle de Contratações - COPLAC
 Serviço de Planejamento e Controle – SEPCO

ATESTADO DE CAPACIDADE TÉCNICA

ACT n.º: 0041/2020

O **SENADO FEDERAL**, inscrito no CNPJ/MF sob o n.º 00.530.279/0001-15, localizado na Praça dos Três Poderes, em Brasília - DF, CEP n.º 70.165-900, atesta para os devidos fins de habilitação junto a Órgãos Públicos e Entidades Privadas, a pedido da interessada, que a empresa **NCT INFORMÁTICA LTDA**, inscrita no CNPJ 03.017.428/0001-35, com sede na SBS Quadra 02, Bloco “Q”, 8º andar, Ed. João Carlos Saad, Brasília/DF, CEP: 70070-120, Telefone: (61) 3201-0000, e-mail: contratos@nct.com.br, *forneceu Solução de Alta Disponibilidade de Next Generation Firewall e de Solução de Gerenciamento Centralizado e Integrado, de acordo com as informações a seguir:*

PROCESSO N.º: 00200.009604/2015-50

MODALIDADE: Pregão Eletrônico

Nº da Licitação: 0106/2016

CONTRATO: 0029/2017

OBJETO: Contratação de empresa especializada para o fornecimento e instalação de Solução de Alta Disponibilidade de Next Generation Firewall e de Solução de Gerenciamento Centralizado e Integrado para o SENADO FEDERAL, incluindo garantia de funcionamento, atualização de assinaturas de proteção, treinamento operacional e prestação de serviços de suporte técnico local e remoto, 24x7, durante o período de 36 (trinta e seis) meses consecutivos.

VIGÊNCIA: Início: 10/05/2017 **Final:** 09/05/2020

Especificação do Objeto (conforme Edital)

1. ESPECIFICAÇÕES

1.1. **ITEM I:** Solução de alta disponibilidade de *Next Generation Firewall*, com garantia de funcionamento, atualização de assinaturas de proteção e suporte técnico local e remoto, 24x7, pelo prazo de 36 (trinta e seis) meses, incluindo serviços de instalação.

1.1.1. Características de hardware por equipamento (appliance)

1.1.1.1. O equipamento deve ser apropriado para o uso em ambiente tropical com umidade relativa na faixa de 10 a 90% (sem condensação) e temperatura ambiente na faixa de 0 a 40°C.

1.1.1.2. O equipamento deve possuir 2 (duas) fontes de alimentação independentes, redundantes e hot-swappable, com alimentação nominal de 100~120VAC e 210~230VAC e frequência de 50 ou 60 Hz, ou auto-ranging. Deverá vir acompanhado



SENADO FEDERAL

Secretaria de Administração de Contratações – SADCON
 Coordenação de Planejamento e Controle de Contratações - COPLAC
 Serviço de Planejamento e Controle – SEPCO

de cabo de alimentação com, no mínimo, 1,80m (6 pés), com plug tripolar 2P+T no padrão ABNT NBR 14136.

- 1.1.1.3. O equipamento deve vir acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc.) para fixação em bastidor (rack) padrão EIA-310 com largura de 19" (dezenove polegadas).
- 1.1.1.4. O equipamento deve possuir, no mínimo, 4 (quatro) interfaces 10 (dez) Gigabit-Ethernet padrão SFP+, com transceivers SFP+ 10GB-LR, para conexão ao meio via cabos de fibra ótica.
- 1.1.1.5. O equipamento deve possuir, no mínimo, 4 (quatro) interfaces 1 (um) Gigabit-Ethernet padrão SFP, com transceivers SFP 1GB-LC-LX, para conexão ao meio via cabos de fibra ótica.
- 1.1.1.6. O equipamento deve possuir, no mínimo, 8 (oito) interfaces 1 (um) Gigabit-Ethernet padrão 1000Base-T, para conexão ao meio via cabos de cobre.
- 1.1.1.7. O equipamento deve possuir 1 (uma) porta de console para configuração e gerenciamento por interface de linha de comando (CLI).
- 1.1.1.8. O equipamento deve possuir, no mínimo, 1 (uma) interface dedicada para gerenciamento, além das interfaces descritas nos itens 2.1.1.4, 2.1.1.5, 2.1.1.6 e 2.1.1.7.
- 1.1.1.9. O equipamento deve possuir, no mínimo, 1 (uma) interface dedicada para o sincronismo de estados da solução de alta disponibilidade, além das interfaces descritas nos itens 2.1.1.4, 2.1.1.5, 2.1.1.6, 2.1.1.7 e 2.1.1.8.
- 1.1.1.10. O equipamento deve possuir, no mínimo, 16GB de memória RAM.
- 1.1.1.11. O equipamento deve possuir, no mínimo, 2 (duas) unidades de armazenamento interno redundantes, com capacidade mínima de 240GB (duzentos e quarenta gigabytes) cada.
- 1.1.1.12. O equipamento deve ser fornecido em sua capacidade máxima de processamento, memória e armazenamento interno.
- 1.1.1.13. O equipamento deve ser fornecido com todas as suas portas de comunicação, interfaces e afins habilitadas, operacionais e prontas para operação, inclusive com seus respectivos transceivers instalados, sem custos adicionais.
- 1.1.1.14. O equipamento deve possuir certificação de conformidade sustentável de acordo com os padrões EPA (Environmental Protection Agency) ou similares, tais como EnergyStar, RoHS (Restriction on Hazardous Substances) ou WEEE (Waste Electrical and Electronic Equipment).

1.1.2. Características de capacidade por equipamento (appliance)

- 1.1.2.1. Taxa de transferência (throughput) mínima de 4 (quatro) Gbps com as funcionalidades de firewall, identificação de usuários, identificação dos países de origem e destino das comunicações (geolocalização), controle de acesso à Internet (controle de aplicações e filtragem de URL's), prevenção contra ameaças (IPS, Antivirus, Anti-Bot, Anti-Malware, Anti-Spyware), administração de largura de banda





SENADO FEDERAL

Secretaria de Administração de Contratações – SADCON
 Coordenação de Planejamento e Controle de Contratações - COPLAC
 Serviço de Planejamento e Controle – SEPCO

de serviço (QoS), descriptografia e inspeção de tráfego SSL, suporte para conexões VPN IPSec e SSL habilitadas simultaneamente.

- 1.1.2.2. Taxa de transferência (throughput) mínima de 2.000.000 (dois milhões) de pacotes por segundo (PPS).
- 1.1.2.3. Mínimo de 2.000.000 (dois milhões) de conexões simultâneas.
- 1.1.2.4. Mínimo de 120.000 (cento e vinte mil) novas conexões por segundo.
- 1.1.2.5. As taxas de transferência acima indicadas devem ser alcançadas com a inspeção integral de todos os pacotes de dados, independentemente de seu tamanho ou direção de fluxo, sem prejuízo na performance do equipamento, e com todas as assinaturas, listas e demais métodos de controle de acesso e de detecção e prevenção de ameaças habilitados.
- 1.1.2.6. As taxas de transferência e quantidades de conexões acima indicadas devem ser alcançadas durante a realização de “teste de bancada”, baseado na RFC-3511 e descrito no Capítulo 11 do edital, que utilizará padrão de tráfego de dados similar ao encontrado nos links de internet do Senado Federal (a partir de dados estatísticos previamente coletados), principalmente no que diz respeito à distribuição de protocolos, conexões e tamanhos de pacotes de dados.

1.1.3. Funcionalidades básicas por equipamento (appliance)

- 1.1.3.1. Deve suportar os protocolos IPv4 e IPv6.
- 1.1.3.2. Deve suportar VLAN's no padrão 802.1q.
- 1.1.3.3. Deve suportar agregação de links no padrão 802.3ad.
- 1.1.3.4. Deve suportar flow control no padrão 802.3x
- 1.1.3.5. Deve suportar os protocolos DHCP e DHCPv6.
- 1.1.3.6. Deve suportar o protocolo NTP.
- 1.1.3.7. Deve suportar as funcionalidades de roteamento estático e dinâmico, em IPv4 e IPv6.
- 1.1.3.8. Deve suportar os protocolos RIP, OSPF v2, OSPF v3 e BGP v4.
- 1.1.3.9. Deve suportar os protocolos IGMP v2, IGMP v3 e PIM-SM.
- 1.1.3.10. Deve suportar os protocolos SNMP v2c e SNMP v3.
- 1.1.3.11. Deve possuir MIB própria contemplando, no mínimo, indicadores de estado do hardware e de performance do equipamento.
- 1.1.3.12. Deve suportar policy based routing (PBR), possibilitando políticas de roteamento condicionado ao endereço IP de origem, endereço IP de destino e porta de comunicação.
- 1.1.3.13. Deve suportar o funcionamento nos modos sniffer (para inspeção de tráfego gerado por uma porta de rede espelhada), layer-2, layer-3 e suas combinações.
- 1.1.3.14. Deve permitir o acesso ao equipamento via CLI (console), SSH e interface web HTTPS.
- 1.1.3.15. Deve possuir funcionalidade de backup/restore de sua configuração e políticas de segurança.
- 1.1.3.16. Deve permitir o agendamento automático dos backups.





SENADO FEDERAL

Secretaria de Administração de Contratações – SADCON
 Coordenação de Planejamento e Controle de Contratações - COPLAC
 Serviço de Planejamento e Controle – SEPCO

1.1.3.17. Deve armazenar os backups localmente, ou na solução de gerenciamento centralizado, e permitir que sejam transferidos para equipamentos externos por meio dos protocolos FTP e SCP.

1.1.3.18. Deve criptografar e autenticar a comunicação com a solução de gerenciamento centralizado.

1.1.4. Funcionalidades de identificação de usuários por equipamento (appliance)

1.1.4.1. Deve promover a integração com serviços de diretório LDAP e Active Directory, baseados em caracteres da língua portuguesa, para a identificação, autenticação, autorização e registro de eventos de acessos ou ameaças.

1.1.4.2. Deve identificar de forma transparente os usuários autenticados por meio de serviço de diretório Microsoft Active Directory, e de servidores RADIUS Microsoft Network Policy Server e Aruba ClearPass Policy Manager.

1.1.4.3. Não será permitida a utilização de agentes instalados nos servidores LDAP, Active Directory, RADIUS, Kerberos e proxies internos, e nem nos equipamentos dos usuários.

1.1.4.4. Não será permitida a interceptação ou espelhamento do tráfego destinado aos servidores LDAP, Active Directory, RADIUS, Kerberos e proxies internos.

1.1.4.5. Será permitido que a solução de gerenciamento centralizado possua um “appliance virtual” específico para atendimento às necessidades de identificação e autenticação de usuários.

1.1.4.6. Deve possuir portal de autenticação (captive portal) para a identificação e autenticação de usuários não registrados ou não reconhecidos por meio dos serviços indicados no item 2.1.4.2.

1.1.4.7. O portal de autenticação deve ser capaz de identificar e autenticar usuários cadastrados em serviço de diretório LDAP e Active Directory.

1.1.4.8. Deve permitir a criação de políticas de segurança baseadas em usuários e grupos de usuários pertencentes a um diretório LDAP ou ao Active Directory.

1.1.4.9. Deve registrar a identificação do usuário em todos os logs de eventos de acesso ou de ameaças gerados pelo equipamento.

1.1.4.10. Deve registrar os eventos dos usuários em tempo real, sem a utilização de processos em lote (batches) ou processos de correlação após a ocorrência do evento em questão.

1.1.4.11. Deve estar licenciado e permitir a identificação e autenticação de pelo menos 10.000 (dez mil) usuários simultâneos.

1.1.5. Funcionalidades de firewall por equipamento (appliance)

1.1.5.1. Não deve possuir restrições ao número de máquinas ou usuários protegidos.

1.1.5.2. Deve suportar a implementação tanto em modo transparente (layer-2) quanto em modo gateway (layer-3).

1.1.5.3. Deve suportar statefull inspection de tráfego IPv4 e IPv6.





SENADO FEDERAL

Secretaria de Administração de Contratações – SADCON
 Coordenação de Planejamento e Controle de Contratações - COPLAC
 Serviço de Planejamento e Controle – SEPCO

- 1.1.5.4. Deve suportar controle de acesso para pelo menos 150 serviços e protocolos pré-definidos.
- 1.1.5.5. Deve suportar os protocolos H.323, SIP, SCCP e MGCP.
- 1.1.5.6. Deve suportar os protocolos MMS, RTCP, RTMP, RTSP e RTP.
- 1.1.5.7. Deve implementar mecanismo de conversão de endereços NAT (Network Address Translation), de forma a possibilitar a realização de 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).
- 1.1.5.8. Deve suportar NAT64.
- 1.1.5.9. Deve permitir o registro de eventos de NAT com as informações de endereço interno, endereço público, data e hora do evento, portas de origem e destino.
- 1.1.5.10. Deve implementar mecanismo de proteção contra ataques de falsificação de endereços IP (anti-spoofing), tanto para IPv4 quanto para IPv6.
- 1.1.5.11. Deve implementar mecanismo de captura de pacotes.
- 1.1.5.12. Deve identificar os usuários para qualquer protocolo ou aplicação baseada em TCP/UDP/ICMP, na forma do item 2.1.4.
- 1.1.5.13. Deve suportar a utilização simultânea de políticas de segurança em IPv4 e IPv6.
- 1.1.5.14. Deve suportar a implementação de políticas de segurança baseadas em: portas, protocolos, usuários, grupos de usuários, endereços IP, redes CIDR/VLSM, horário ou período de tempo, e suas combinações.
- 1.1.5.15. Deve aplicar novas políticas de segurança sem provocar indisponibilidade de serviço ou descontinuidade das conexões ativas.
- 1.1.5.16. Deve possibilitar o registro dos fluxos de dados relativos a cada sessão, armazenando: endereços IP de origem e destino dos pacotes, traduções NAT, portas e protocolos de origem e destino, usuário identificado, número sequencial dos pacotes TCP e UDP, status dos flags "ACK", "SYN" e "FIN", ação sobre o pacote (permitido ou negado).

1.1.6. Funcionalidades de geolocalização por equipamento (appliance)

- 1.1.6.1. Deve identificar os países de origem e destino de todas as conexões estabelecidas através do equipamento.
- 1.1.6.2. Deve suportar a atualização automática das listas de geolocalização.
- 1.1.6.3. Deve aplicar as atualizações sem perda das conexões ativas.
- 1.1.6.4. Deve armazenar as listas de geolocalização no próprio equipamento.
- 1.1.6.5. Deve permitir a criação de políticas de segurança baseadas em geolocalização, permitindo o bloqueio de tráfego com origem ou destino a determinado país ou grupo de países.
- 1.1.6.6. Deve possibilitar a visualização dos países de origem e destino nos logs de eventos de acessos e ameaças.

1.1.7. Funcionalidades de controle de acesso à Internet por equipamento (appliance)





SENADO FEDERAL

Secretaria de Administração de Contratações – SADCON
 Coordenação de Planejamento e Controle de Contratações - COPLAC
 Serviço de Planejamento e Controle – SEPCO

- 1.1.7.1. Deve prover o controle e proteção de acesso à Internet por meio do reconhecimento de aplicações, independente de porta e protocolo, e da classificação de URLs.
- 1.1.7.2. Deve ser capaz de identificar aplicações, independentemente das portas e protocolos, bem como das técnicas de evasão utilizadas.
- 1.1.7.3. Deve ser capaz de identificar se as aplicações estão utilizando sua porta default.
- 1.1.7.4. Deve ser capaz de identificar aplicações encapsuladas dentro de protocolos, como HTTP e HTTPS.
- 1.1.7.5. Deve ser capaz de identificar aplicações criptografadas usando SSL.
- 1.1.7.6. Deve ser capaz de identificar um mínimo de 2.000 (duas mil) aplicações, incluindo, mas não se limitando a: peer-to-peer, streaming e download de áudio, streaming e download de vídeo, update de software, instant messaging, redes sociais, proxies, anonymizers, acesso e controle remoto, VOIP e email.
- 1.1.7.7. Deve ser capaz de identificar, no mínimo, as seguintes aplicações: Bittorrent, Youtube, Livestream, Skype, Viber, WhatsApp, Snapchat, Facebook, Facebook Messenger, Google+, Google Talk, Tinder, Instagram, Twitter, Linkedin, Dropbox, Google Drive, One Drive, Logmein, Teamviewer, MS-RDP, VNC, Ultrasurf, TOR, Webex.
- 1.1.7.8. Deve permitir a criação de assinaturas para identificação de aplicações proprietárias do órgão, sem a necessidade de ação ou intervenção do fabricante.
- 1.1.7.9. Deve suportar a atualização automática da base de assinaturas utilizada na identificação das aplicações.
- 1.1.7.10. Deve aplicar as atualizações sem perda das conexões ativas.
- 1.1.7.11. Deve armazenar a base de assinaturas no próprio equipamento.
- 1.1.7.12. Deve classificar as aplicações em categorias, tecnologia e fator de risco.
- 1.1.7.13. Deve identificar os usuários que estão utilizando as aplicações, na forma do item 2.1.4.
- 1.1.7.14. Deve permitir o bloqueio de aplicações que não estejam utilizando suas portas default.
- 1.1.7.15. Deve suportar a implementação de políticas de segurança baseadas em: aplicações, categorias de aplicações, fator de risco, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações.
- 1.1.7.16. Deve permitir a utilização ou bloqueio individualizado das aplicações, como BitTorrent e Skype, para determinados usuários ou grupos de usuários.
- 1.1.7.17. Deve permitir registrar todos os fluxos autorizados/bloqueados das aplicações, incluindo o usuário identificado.
- 1.1.7.18. Deve alertar o usuário quando uma aplicação for bloqueada.
- 1.1.7.19. Deve permitir o controle de uso de banda de download ou upload utilizada pelas aplicações (traffic shaping) baseado em: endereço IP ou rede CIDR/VLSM de origem





SENADO FEDERAL

Secretaria de Administração de Contratações – SADCON
 Coordenação de Planejamento e Controle de Contratações - COPLAC
 Serviço de Planejamento e Controle – SEPCO

ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações.

- 1.1.7.20. Deve ser capaz de efetuar a classificação de conteúdo de páginas web em HTTP e HTTPS, baseado em listas de categoria.
- 1.1.7.21. Deve possuir no mínimo 60 categorias de URLs, incluindo, mas não se limitando, as seguintes categorias ou suas semelhantes: adult, chat, drugs, gambling, games, hacking, hate speech, remote proxies, social networks, streaming media, violence, weapons.
- 1.1.7.22. Deve permitir sobrescrever as categorias de uma URL que se considere indevidamente classificada.
- 1.1.7.23. Deve permitir a criação de categorias customizadas.
- 1.1.7.24. Deve permitir a inclusão de URLs customizadas nas categorias já existentes ou previamente customizadas.
- 1.1.7.25. Deve suportar a atualização automática das listas de categorias.
- 1.1.7.26. Deve aplicar as atualizações sem perda das conexões ativas.
- 1.1.7.27. Deve armazenar as listas de categoria no próprio equipamento.
- 1.1.7.28. Deve identificar os usuários que estão acessando as páginas web, na forma do item 2.1.4.
- 1.1.7.29. Deve suportar a implementação de políticas de segurança baseadas em: URLs, categorias de URLs, fator de risco, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações
- 1.1.7.30. Deve alertar o usuário quando uma URL for bloqueada, por meio de página de bloqueio que possa ser customizada no próprio equipamento, e que informe, no mínimo, o motivo do bloqueio e a categoria na qual a URL foi classificada.
- 1.1.7.31. Deve permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado, informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para possibilitar o usuário continuar acessando o site).
- 1.1.7.32. Deve permitir registrar todos os acessos autorizados ou bloqueados às páginas web, incluindo sua classificação e o usuário identificado.

1.1.8. Funcionalidades de prevenção de ameaças por equipamento (appliance)

- 1.1.8.1. Deve possuir, no mínimo, funcionalidades de IPS, Antivirus, Anti-Bot, Anti-Malware e Anti-Spyware
- 1.1.8.2. Deve possuir, no mínimo, os seguintes mecanismos de detecção: assinaturas de vulnerabilidades e exploits, assinaturas de ataques, validação de protocolos, detecção de anomalias, IP defragmentation, remontagem de pacotes TCP, detecção baseada em comportamento, nível de severidade do ataque e nível de confiança de detecção do ataque.
- 1.1.8.3. Deve possuir proteção contra ataques de negação de serviço DoS e DDoS.
- 1.1.8.4. Deve possuir assinaturas para bloqueio de ataques "buffer overflow".





SENADO FEDERAL

Secretaria de Administração de Contratações – SADCON
 Coordenação de Planejamento e Controle de Contratações - COPLAC
 Serviço de Planejamento e Controle – SEPCO

- 1.1.8.5. Deve possuir mecanismo automático de captura de pacotes de eventos de IPS, para fins de troubleshooting e análise forense.
- 1.1.8.6. Deve ser capaz de inspecionar tráfego criptografado usando SSL.
- 1.1.8.7. Deve ser capaz de inspecionar integralmente todos os pacotes de dados, independentemente de seus tamanhos, sem prejuízo na performance do equipamento, até os limites indicados no item 2.1.2.
- 1.1.8.8. Deve possuir referência cruzada da base de assinaturas de detecção com os identificadores CVE (Common Vulnerabilities and Exposures).
- 1.1.8.9. Deve possibilitar a criação de assinaturas customizadas.
- 1.1.8.10. Deve identificar os usuários relacionados aos eventos de IPS, na forma do item 2.1.4.
- 1.1.8.11. Deve permitir a criação de políticas de segurança que alertem, sem bloquear, sobre a ocorrência de um determinado ataque, com origem/destino em determinado endereço IP/rede CIDR.
- 1.1.8.12. Deve permitir a criação de políticas de segurança que bloqueiem um determinado ataque por meio de uma ação de DROP/RESET, com origem/destino em determinado endereço IP/rede CIDR.
- 1.1.8.13. Deve permitir a criação de exceções/exclusões de inspeção de uma determinada assinatura ou grupo de assinaturas, com origem/destino em determinado endereço IP/rede CIDR.
- 1.1.8.14. Deve permitir registrar todos os eventos de IPS, incluindo o usuário identificado.
- 1.1.8.15. Deve identificar e bloquear a comunicação com botnets.
- 1.1.8.16. Deve bloquear malwares e spywares.
- 1.1.8.17. Deve inspecionar e bloquear vírus nos seguintes tipos de tráfego, no mínimo: HTTP, HTTPS e SMTP.
- 1.1.8.18. Deve suportar proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.
- 1.1.8.19. Deve suportar a inspeção de vírus em arquivos comprimidos utilizando o algoritmo deflate (zip, gzip, etc.).
- 1.1.8.20. Deverá suportar bloqueio de download de pelo menos 45 tipos de arquivos.
- 1.1.8.21. Deverá suportar bloqueio de download de pelo menos 50 tipos de arquivos.
- 1.1.8.22. Deve suportar a atualização automática das bases de assinaturas.
- 1.1.8.23. Deve aplicar as atualizações sem reboot do equipamento e nem perda das conexões ativas.
- 1.1.8.24. Deve armazenar as bases de assinaturas no próprio equipamento.
- 1.1.8.25. Deve identificar os usuários relacionados aos eventos de bloqueio, na forma do item 2.1.4.
- 1.1.8.26. Deve permitir a criação de políticas de segurança que alertem, sem bloquear, sobre a ocorrência de uma determinada ameaça, com origem/destino em determinado endereço IP/rede CIDR.





SENADO FEDERAL

Secretaria de Administração de Contratações – SADCON
 Coordenação de Planejamento e Controle de Contratações - COPLAC
 Serviço de Planejamento e Controle – SEPCO

1.1.8.27. Deve permitir a criação de políticas de segurança que bloqueiem uma determinada ameaça, com origem/destino em determinado endereço IP/rede CIDR.

1.1.8.28. Suportar notificações e alertas via email, SNMP traps e log de pacotes.

1.1.9. Características de QoS por equipamento (appliance)

1.1.9.1. Deve permitir o controle de políticas de uso com base nas aplicações: permitir, negar, agendar, inspecionar e controlar o uso da largura de banda que utilizam cada aplicação ou usuário.

1.1.9.2. Deve suportar a criação de políticas de controle de uso de largura de banda baseadas em: porta ou protocolo, endereço IP de origem ou destino, usuário ou grupo de usuários, aplicações (por exemplo, Youtube e WhatsApp).

1.1.9.3. Deve suportar a priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP e MGCP.

1.1.9.4. Deve suportar a marcação de pacotes DiffServ.

1.1.9.5. Deve permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

1.1.10. Características de inspeção SSL por equipamento (appliance)

1.1.10.1. Deve identificar, decryptografar e analisar o tráfego SSL tanto em conexões de entrada (Inbound) quanto de saída (Outbound).

1.1.10.2. Deve permitir a decryptografia da área útil do pacote de dados (payload) para fins de controle de acesso à Internet e proteção contra ameaças.

1.1.10.3. Deve permitir a diferenciação de conexões pessoais (Bancos, Shopping, etc.) e conexões não pessoais por meio de classificação automática.

1.1.11. Características de VPN por equipamento (appliance)

1.1.11.1. Deve disponibilizar licenciamento para VPN site-to-site e client-to-site, sem limite do número de usuários simultâneos e sem limite do uso de túneis, respeitando o limite previsto no item 2.1.2.5.

1.1.11.2. Deve suportar, no mínimo, 4.000 (quatro mil) túneis VPN IPSec simultâneos.

1.1.11.3. Deve suportar, no mínimo, 5.000 (cinco mil) usuários VPN SSL.

1.1.11.4. Deve suportar VPN site-to-site em topologia Full Meshed (todos os gateways possuem links específicos para todos os demais gateways) e Estrela (gateways satélites se comunicam somente com um único gateway central).

1.1.11.5. Deve suportar criptografia 3DES, AES-128, AES-256.

1.1.11.6. Deve suportar integridade de dados com MD5, SHA-1 e SHA-256.

1.1.11.7. Deve suportar o protocolo IKE, fases I e II.

1.1.11.8. Deve suportar os algoritmos RSA e Diffie-Hellman groups 1, 2, 5 e 14.

1.1.11.9. Deve suportar NAT-T (NAT Traversal).

1.1.11.10. Deve suportar VPN IPSec client-to-site.

1.1.11.11. Deve possuir cliente próprio para instalação nos dispositivos móveis dos usuários, sem custo adicional e sem limite do número de usuários.





SENADO FEDERAL

Secretaria de Administração de Contratações – SADCON
 Coordenação de Planejamento e Controle de Contratações - COPLAC
 Serviço de Planejamento e Controle – SEPCO

- 1.1.11.12. O cliente de VPN client-to-site deve ser compatível ou suportar o cliente nativo de pelo menos: Windows XP, Windows Vista (32 e 64 bits), Windows 7 (32 e 64 bits), Windows 8 (32 e 64 bits), Windows 8.1 (32 e 64 bits), Windows 10 (32 e 64 bits), Apple IOS, Android, Mac OSx 10 e Linux.
 - 1.1.11.13. Deve suportar atribuição de endereço IP nos clientes remotos de VPN.
 - 1.1.11.14. Deve suportar atribuição de DNS nos clientes remotos de VPN.
 - 1.1.11.15. Deve suportar, no mínimo, os protocolos de roteamento estático e dinâmico OSPF ou BGP.
 - 1.1.11.16. O túnel VPN do cliente ao gateway (client-to-site) deve fornecer uma solução de autenticação única (single-sign-on) aos usuários, integrando-se com as ferramentas de Windows login.
 - 1.1.11.17. Deve permitir criar políticas por usuário e grupos para tráfego de VPN client-to-site.
 - 1.1.11.18. Deve suportar autoridade certificadora integrada ao gateway VPN ou à solução de gerenciamento centralizado.
 - 1.1.11.19. Deve promover a integração com diretórios LDAP e Active Directory para a autenticação de usuários de VPN e regras de acesso.
 - 1.1.11.20. Deve suportar os métodos de autenticação de VPN: usuário e senha de base interna do próprio equipamento, usuário e senha de diretório LDAP, usuário e senha do Active Directory, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao equipamento ou à solução de gerenciamento centralizado, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao Active Directory, certificação digital por meio de certificados emitidos por autoridade certificadora no padrão ICP-Brasil.
 - 1.1.11.21. Deve suportar a integração com autoridades certificadoras de terceiros que possam gerar certificados no formato PKCS#12.
 - 1.1.11.22. Deve suportar a solicitação de emissão de certificados à uma autoridade certificadora de confiança (enrollment) via SCEP (Simple Certificate Enrollment Protocol) ou CSR (Certificate Signing Requests).
 - 1.1.11.23. Deve suportar a leitura e verificação de CRLs (certification revocation lists).
 - 1.1.11.24. Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis de SSL.
- 1.1.12. Características de alta disponibilidade**
- 1.1.12.1. Deve operar em alta disponibilidade (HA) nativamente no equipamento, permitindo uma arquitetura ativo/ativo e ativo/passivo com no mínimo 2 (dois) membros, com sincronismo de estados integrado.
 - 1.1.12.2. Deve suportar o balanceamento de carga interno na arquitetura ativo/ativo.
 - 1.1.12.3. Deve sincronizar: todas as configurações, sessões TCP/IP, tabelas NAT, listas e assinaturas utilizadas para controle de acesso à Internet e proteção contra ameaças, tabelas FIB, associações de segurança das VPNs.
 - 1.1.12.4. Deve monitorar a falha dos links de comunicação.





SENADO FEDERAL

Secretaria de Administração de Contratações – SADCON
 Coordenação de Planejamento e Controle de Contratações - COPLAC
 Serviço de Planejamento e Controle – SEPCO

1.1.12.5. Deve ser capaz de identificar e iniciar automaticamente um procedimento de failover sempre que ocorrer: a falha de um dos membros do cluster, a falha de qualquer componente ou processo crítico de um dos membros do cluster, a falha de um dos links de comunicação monitorados.

1.1.12.6. Deve ser capaz de realizar os procedimentos de failover sem perda das conexões ativas, interrupções de tráfego.

1.2. ITEM II – Solução de gerenciamento centralizado e integrado, com garantia de funcionamento, atualização de assinaturas de proteção e suporte técnico local e remoto, 24x7, pelo prazo de 36 (trinta e seis) meses, incluindo serviços de instalação.

1.2.1. Funcionalidades da gerência centralizada

1.2.1.1. A solução deve ser do tipo “appliance virtual” – solução de software baseada em máquina virtual, conforme os padrões estabelecidos pelo DMTF (Distributed Management Task Force), ou sistema operacional desenvolvido pelo próprio fabricante da solução de gerenciamento que possa ser instalado e executado em ambiente virtual – compatível com VMware vSphere 5.5 ou superior.

1.2.1.2. Deve estar licenciada e permitir a gerência centralizada de todos os equipamentos e contextos virtuais que compõem a solução de alta disponibilidade.

1.2.1.3. Deve estar licenciada para o limite máximo de usuários, objetos, regras de segurança, NAT e endereços IP suportados pela solução.

1.2.1.4. Deve estar licenciada e permitir a correlação de todos os eventos gerados por todos os equipamentos e contextos virtuais que compõe a solução de alta disponibilidade.

1.2.1.5. Deve permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras em todos os clusters.

1.2.1.6. Deve suportar, por meio da interface gráfica de gerenciamento, a criação e administração de políticas de Next Generation Firewall, filtragem de URLs, monitoração de logs, debugging, troubleshooting e captura de pacotes.

1.2.1.7. Deve possuir a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura.

1.2.1.8. Deve permitir, de forma granular, assinalar permissões para os administradores criarem outros usuários, alterarem configurações, ler configurações, etc.

1.2.1.9. Deve permitir a delegação de funções de administração.

1.2.1.10. Deve suportar o bloqueio de alterações, evitando o conflito de configurações entre diferentes administradores efetuando alterações simultaneamente.

1.2.1.11. Deve registrar em log de auditoria as ações dos usuários administradores.

1.2.1.12. Deve suportar a identificação e utilização de usuários nas políticas de segurança, na forma do item 2.1.4.

1.2.1.13. Deve suportar agrupamento lógico de objetos ("object grouping") para criação de regras.

1.2.1.14. Deve possibilitar o gerenciamento (incluindo a criação, alteração, monitoração e exclusão) de objetos de rede. Deverá ainda permitir detectar se e onde, na base de





SENADO FEDERAL

Secretaria de Administração de Contratações – SADCON
 Coordenação de Planejamento e Controle de Contratações - COPLAC
 Serviço de Planejamento e Controle – SEPCO

regras, está sendo utilizado determinado objeto de rede. Os tipos de objetos deverão permitir especificar de forma distinta grupos e objetos de rede e serviços, diferenciando-os e agrupando-os conforme suas características ou descrição de maneira a permitir o reaproveitamento dos mesmos em diferentes políticas.

- 1.2.1.15. Deve contabilizar a utilização ("hit counts") ou o volume de dados trafegados correspondente a cada regra de filtragem ("Access Control Entry") individualmente.
- 1.2.1.16. Deve 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).
- 1.2.1.17. Deve permitir distribuição centralizada de pacotes de atualização.
- 1.2.1.18. Deve ser capaz de testar a conectividade dos equipamentos gerenciados.
- 1.2.1.19. Deve suportar configuração das funcionalidades de alta disponibilidade dos dispositivos físicos.
- 1.2.1.20. Deve permitir localizar em quais regras um objeto está sendo utilizado.
- 1.2.1.21. Deve 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.
- 1.2.1.22. Deve 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).
- 1.2.1.23. Deve suportar a geração de alertas automáticos via email, SNMP e syslog.
- 1.2.1.24. Deve suportar rollback de configuração para a última configuração salva.
- 1.2.1.25. Deve permitir validar as regras antes de aplicá-las.
- 1.2.1.26. Deve permitir a visualização e comparação das configurações atual, anterior e antigas.
- 1.2.1.27. Deve permitir a exportação automática e agendada de logs via SCP.
- 1.2.1.28. Deve informar a utilização dos recursos de CPU, memória, armazenamento interno e atividade de rede dos equipamentos gerenciados.
- 1.2.1.29. Deve informar o número de conexões simultâneas e de novas conexões por segundo dos equipamentos gerenciados.
- 1.2.1.30. Deve possuir relatórios de utilização dos recursos por aplicação, URLs, ameaças, etc.
- 1.2.1.31. Deve possuir visualização sumarizada de todas as aplicações, ameaças e URLs que foram identificadas e controladas pela solução.
- 1.2.1.32. Deve permitir a criação de relatórios customizados.
- 1.2.1.33. Deve possibilitar a filtragem dos logs do equipamento por, no mínimo: aplicação, endereço IP de origem e destino, país de origem e destino, usuário e horário.
- 1.2.1.34. Deve possuir relatórios com informações consolidadas sobre: as mais frequentes fontes de conexões bloqueadas com seus destinos e serviços, os mais frequentes ataques e ameaças de segurança detectados com suas origens e destinos, os serviços de rede mais utilizados, as aplicações maiores consumidoras de banda de Internet, os





SENADO FEDERAL

Secretaria de Administração de Contratações – SADCON
 Coordenação de Planejamento e Controle de Contratações - COPLAC
 Serviço de Planejamento e Controle – SEPCO

usuários maiores consumidores de banda de Internet, os sítios na Internet mais visitados.

1.2.1.35. Deve permitir a geração automática e agendada dos relatórios.

1.2.1.36. Deve estar licenciada para receber pelo menos 10.000 (dez mil) registros de log por segundo e 100GBytes de logs diários.

1.2.1.37. Deve permitir a utilização de pelo menos 10TBytes de espaço em disco

1.3. ITEM III: Transferência de Conhecimentos e Workshops de atualização de conhecimentos

1.3.1. Treinamento personalizado

1.3.1.1. Os treinamentos deverão ser realizados e concluídos para até 8 (oito) servidores do PRODASEN, divididos em 2 (duas) turmas separadas, ambas dentro de prazo máximo de 120 (cento e vinte) dias corridos, a contar da data de assinatura do contrato, de acordo com cronograma estabelecido entre a Equipe Técnica do PRODASEN e a Contratada, e deverão ser ministrados por instrutores preparados e certificados pelo fabricante dos produtos, em centros de treinamento certificados pelo fabricante — com infraestrutura de hardware, software, laboratório de testes e material didático — cumprindo o programa oficial de treinamento do fabricante, inclusive com aulas práticas e teóricas.

1.3.1.2. Caso seja de interesse do Senado Federal, o treinamento poderá ser realizado em turma única de até 8 (oito) servidores do PRODASEN.

1.3.1.3. O cronograma para realização dos treinamentos deverá ser proposto pela Contratada, em prazo máximo de 20 (vinte) dias corridos, contados da assinatura do contrato. O PRODASEN analisará o cronograma, estabelecendo posteriormente, em até 5 (cinco) dias úteis, as datas definitivas com a Contratada.

1.3.1.4. A Contratada deverá apresentar descrição completa e detalhada das instalações onde serão realizados os treinamentos, que deverão ser previamente aprovadas pelo PRODASEN, juntamente com o cronograma de realização, no prazo estabelecido no item 2.3.1.3.

1.3.1.5. Os treinamentos deverão ter carga horária mínima de 40 (quarenta) horas, cobrindo conteúdo teórico e prático, em nível avançado e personalizado para a solução fornecida, incluindo tópicos e cenários avançados de arquitetura, instalação, configuração, operação e resolução de problemas.

1.3.1.6. O curso e o material didático deverão estar, preferencialmente, em língua portuguesa, ou, na sua impossibilidade, em língua inglesa.

1.3.1.7. Caso os treinamentos sejam realizados fora de Brasília/DF, despesas com transporte (aéreo e local), hospedagem e alimentação deverão ser custeadas pela Contratada.

1.3.1.8. Os treinamentos serão avaliados por cada grupo, e caso não obtenham nota mínima 3 (três) de um máximo de 5 (cinco), fica a Contratada obrigada a realizar novo treinamento, dentro de 60 (sessenta) dias corridos, sem ônus adicional para o Senado Federal, corrigindo as deficiências apontadas na avaliação.





SENADO FEDERAL

Secretaria de Administração de Contratações – SADCON
 Coordenação de Planejamento e Controle de Contratações - COPLAC
 Serviço de Planejamento e Controle – SEPCO

- 1.3.1.9. Deverão ser emitidos certificados de conclusão dos treinamentos para todos os participantes. O prazo para emissão e envio dos certificados aos alunos é de 30 (trinta) dias corridos após o término de cada curso.
- 1.3.1.10. Após a realização de cada treinamento, será emitido um Termo de Aceite do Treinamento, em até 15 (quinze) dias corridos a contar da conclusão do treinamento de cada turma.

Workshop de atualização de conhecimentos

- 1.3.1.11. A Contratada deverá realizar 2 (dois) Workshops de Atualização de Conhecimentos, para até 8 (oito) servidores do PRODASEN cada.
- 1.3.1.12. Cada workshop deverá ser concluído até 90 (noventa) dias corridos após a data de término de cada ciclo anual do contrato, considerando a data de assinatura do contrato como o início do primeiro ciclo anual, de acordo com cronograma estabelecido entre a Equipe Técnica do PRODASEN e a Contratada.
- 1.3.1.13. Os Workshops poderão ser realizados nas dependências do PRODASEN ou nas dependências indicadas pela Contratada, e deverão ser ministrados por instrutores preparados e certificados pelo fabricante dos produtos.
- 1.3.1.14. O cronograma para realização dos workshops deverá ser proposto pela Contratada, até 30 (trinta) dias corridos após o término de cada ciclo anual do contrato, considerando a data de assinatura do contrato como o início do primeiro ciclo anual. O PRODASEN analisará o cronograma, estabelecendo posteriormente, em até 5 (cinco) dias úteis, as datas definitivas com a Contratada.
- 1.3.1.15. Os workshops deverão ter carga horária mínima de 8 (oito) horas, cobrindo conteúdo teórico e prático, em nível avançado e personalizado para a solução fornecida, com foco nas atualizações aplicadas à solução durante cada ciclo anual, bem como em tópicos de interesse da Equipe Técnica do PRODASEN.
- 1.3.1.16. O workshop e o material didático deverão estar, preferencialmente, em língua portuguesa, ou, na sua impossibilidade, em língua inglesa.
- 1.3.1.17. Caso os treinamentos sejam realizados fora de Brasília/DF, despesas com transporte (aéreo e local), hospedagem e alimentação deverão ser custeadas pela Contratada.
- 1.3.1.18. Os workshops serão avaliados por cada grupo, e caso não obtenham nota mínima 3 (três) de um máximo de 5 (cinco), fica a Contratada obrigada a realizar novo workshop, dentro de 30 (trinta) dias corridos, sem ônus adicional para o Senado Federal, corrigindo as deficiências apontadas na avaliação.
- 1.3.1.19. Deverão ser emitidos certificados de conclusão dos workshops para todos os participantes. O prazo para emissão e envio dos certificados aos alunos é de 30 (trinta) dias corridos após o término de cada curso.





SENADO FEDERAL

Secretaria de Administração de Contratações – SADCON
 Coordenação de Planejamento e Controle de Contratações - COPLAC
 Serviço de Planejamento e Controle – SEPCO

Do Regime de Execução (conforme Contrato)

A CONTRATADA deverá entregar e instalar todos os equipamentos componentes da solução objeto deste contrato, no prazo máximo de 90 (noventa) dias corridos, após a assinatura do contrato.

PARÁGRAFO PRIMEIRO - Todos os equipamentos e seus componentes deverão ser novos, sem uso, entregues em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em suas embalagens originais.

PARÁGRAFO SEGUNDO - Cada solução de alta disponibilidade de next generation firewall (item I) terá um dos seus equipamentos instalados no datacenter principal do SENADO, localizado no PRODASEN – Via N2, Anexo “C” do SENADO; e o outro dos seus equipamentos instalado no datacenter redundante, localizado no datacenter da Câmara dos Deputados CETEC Norte – Via N3, Projeção L, Bloco C – Complexo Avançado.

PARÁGRAFO TERCEIRO - A solução de gerenciamento centralizado (item II) será instalada no datacenter principal do SENADO, localizado no PRODASEN – Via N2, Anexo “C” do SENADO.

PARÁGRAFO QUARTO - Efetivada a entrega e a instalação da solução, o objeto será recebido:

- I - provisoriamente, pelo órgão recebedor do objeto, para efeito de posterior verificação da conformidade das especificações; e
- II - definitivamente, pelo gestor responsável pela fiscalização do ajuste ou, nos casos em que se enquadrarem no §8º do art. 15 da Lei nº 8.666/93, por comissão designada pela Diretora-Geral, no prazo máximo de 05 (cinco) dias úteis, contados após o término da instalação da solução no SENADO, mediante termo circunstanciado, após avaliação de conformidade pelo PRODASEN, verificação de que os mesmos estão de acordo com as especificações técnicas estabelecidas e se as demais condições contratuais foram atendidas.

PARÁGRAFO QUINTO - Ao SENADO não caberá qualquer ônus pela rejeição de produtos e/ou serviços considerados inadequados pelo gestor.





SENADO FEDERAL

Secretaria de Administração de Contratações – SADCON
Coordenação de Planejamento e Controle de Contratações - COPLAC
Serviço de Planejamento e Controle – SEPCO

Declaramos que, segundo informações constantes no Documento Digital n.º 00100.071424/2020-82, a empresa supracitada forneceu o objeto do Contrato n.º 2017/0029 de maneira satisfatória, de acordo com as suas especificações, dentro dos prazos e condições contratuais estabelecidos, nada havendo de forma definitiva e irreversível no âmbito do Senado Federal, até a presente data, que possa desaboná-la.

Brasília-DF, 12 de agosto de 2020.

(Assinado Eletronicamente)

RODRIGO GALHA
Diretor da SADCON

(Assinado Eletronicamente)

**ALEXANDRE MATTOS DE
FREITAS**
Coordenador da COPLAC

(Assinado Eletronicamente)

LEONARDO ARRUDA DO AMARAL ANDRADE
Gestor do NGACTI





O documento foi assinado por:

LEONARDO ARRUDA DO AMARAL ANDRADE	13/08/2020 10:01:06	
Alexandre Mattos de Freitas	18/08/2020 09:19:47	
RODRIGO GALHA	19/08/2020 09:29:51	

A assinatura digital deste documento é Válida e Confiável.

Para obter mais informações sobre o certificado usado para assinar digitalmente o documento clique em Detalhes.