Estudo Técnico Preliminar - 93/2022

1. Informações Básicas

Número do processo: 23090.003445/2022-07

2. Descrição da necessidade

Contratação de empresa especializada no fornecimento de solução de segurança da informação (Firewall).

Pretende-se com o Estudo Técnico Preliminar, verificar a forma mais vantajosa de se estabelecer a contratação de empresa especializada no fornecimento de solução de segurança da informação (Firewall) para proteção de acessos à rede LAN (interna) e WAN (externa), no intuito de garantir a confidencialidade, integridade e disponibilidade dos dados transmitidos ou armazenados na infraestrutura de rede da Universidade Federal de Lavras - UFLA, bem como gerenciar os riscos e ameaças aos ativos de tecnologia da informação dessa instituição.

Atualmente, a UFLA utiliza a solução (appliance) de Firewall “Supermassive 9600” da empresa SonicWall, cujas licenças vão expirar na data 19/06/2022. Vale ressaltar que não haverá mais suporte técnico da SonicWall após encerramento das licenças. Todos os serviços de tecnologia da informação podem ser comprometidos caso a solução de firewall não esteja operante, em consequência, os serviços acadêmicos e administrativos, que também dependem de ativos de tecnologia da informação, podem ser prejudicados ou descontinuados.

Além disso, é necessário aprimorar os conhecimentos técnicos da equipe de segurança computacional e segurança da informação em relação à administração da solução de firewall contratada, pois é necessário atualizar os profissionais de tecnologia da informação da DGTI sobre as novas técnicas de administração da solução de firewall contratada, para uso racional do recurso e resposta rápida a incidentes de segurança da informação.

3. Área requisitante

Área Requisitante	Responsável
Coordenadoria de Operação e Segurança da Informação	Fernando Elias de Oliveira

4. Necessidades de Negócio

1	Disponibilidade dos sistemas institucionais.
2	Salvaguarda dos ativos de tecnologia da informação.
3	Continuidade dos processos de negócios.
4	Bloqueio de ataques e conexões estranhas aos serviços de tecnologia da informação da UFLA.

5	Isolamento seguro dos serviços de tecnologia da informação institucionais.

5. Necessidades Tecnológicas

Para maior clareza, as necessidades tecnológicas seguem descritas de acordo com as três possíveis soluções estudadas. A Equipe de Planejamento da Contratação julgou necessário estudar três possíveis soluções/cenários, um cenário de manutenção e dois cenários de ampliação da capacidade do firewall, sendo que uma solução considera a disputa de vários fabricantes e na outra optou-se por manter-se o fabricante atual no sentido de se obter desconto na aquisição de um novo equipamento por meio de atualização tecnológica de hardware/software.

Assim, ficaram as seguintes soluções:

Solução 01: Renovação da licença vigente com aquisição de licença adicional SonicWall Analytics.

Solução 02: Aquisição de novo firewall e suas respectivas licenças e aquisição de licença de software de gerência de logs e relatórios centralizados.

Solução 03: Upgrade do firewall existente (SonicWall Supermassive 9600), renovação das assinaturas vigentes e aquisição de licença adicional SonicWall Analytics.

Identificação das necessidades tecnológicas	
1	**Renovação da licença Advanced Gateway Security Suite (AGSS) com suporte técnico e garantia do appliance de firewall SonicWall Supermassive 9600 em par de Alta Disponibilidade e aquisição da licença SonicWall Analytics Software, ambas pelo período de 24 meses.** **IPS / Gateway AV / Controle de aplicações** IDS interno, capaz de detectar e evitar automaticamente, IP Source Spoofing, IP Source Routing, Tunel IPsec e ataques tipo DoS (Denial-of-Service) como Ping of Death, SYN Flood, LAND Attack, IP Spoofing, com a possibilidade de se atualizar as assinaturas e carregar novas por meio da atualização do software de sistema operacional do equipamento (appliance). Deve implementar assinaturas dinâmicas de IPS (Intrusion Prevention System) capaz de realizar inspeção no campo de "Dados" do pacote IP para detecção e prevenção de ataques. A funcionalidade de IPS deve possuir no mínimo 3.500 (três mil e quinhentas) assinaturas contra ataques, carregadas automaticamente no equipamento quando ativado o serviço. Deve implementar assinaturas dinâmicas de Gateway Antivírus capaz de realizar inspeção no campo de "Dados" do pacote IP para detecção e prevenção de vírus, worms, spywares, malwares, etc. A funcionalidade de Gateway Antivírus deve possuir no mínimo 20.000 (vinte mil) assinaturas contra ataques, carregadas automaticamente no equipamento quando ativado o serviço. Essa funcionalidade não deve possuir limitação de tamanho de arquivo para varredura. Gateway Antivírus deve ser capaz de identificar ameaças nos seguintes protocolos: HTTP, SMTP, POP, IMAP, CIFS/NETBIOS e TCP STREAM. Deve possuir flexibilidade para liberar aplicações da inspeção profunda de pacotes, ou seja, excluir a aplicação da checagem de IPS, Gateway Antivirus/AntiSpyware.

	Deve possuir funcionalidade para bloquear, limitar e garantir banda baseado em assinaturas de aplicações. Deve possuir no mínimo 4.000 (quatro mil) assinaturas de aplicações, carregadas automaticamente no equipamento quando ativado o serviço. Deve permitir a criação de assinaturas customizadas via interface gráfica de gerenciamento. Deve permitir a restrição de arquivos por sua extensão e bloqueio de anexos por meio de protocolos SMTP e POP3 baseado em seus nomes ou tipos mime. Deve permitir a filtragem de e-mails pelo seu conteúdo, por meio da definição de palavras-chave e a sua forma de pesquisa. **Filtro de conteúdo WEB** Deve implementar checagem de URLs requisitadas pelos usuários e classificá-las em categorias para que possam ser bloqueadas, liberadas e/ou ter a utilização de banda customizada. As consultas para categorizar as URLs deverão ser dinâmicas via Internet, utilizando base de dados do mesmo ou de outro fabricante. Deve possuir no mínimo 40 (quarenta) categorias de URL e com, pelo menos, as seguintes categorias: violência, nudismo, roupas intimas / banho, pornografia, armas, ódio / racismo, cultos / ocultismo, drogas / drogas ilegais, crimes / comportamento ilegal, educação sexual, jogos, álcool / tabagismo, conteúdo adulto, conteúdo questionável, artes e entretenimento, bancos / e trading, chat, negócios e economia, tecnologia de computadores e Internet, e-mail pessoal, jogos de azar, hacking, humor, busca de empregos, newsgroups, encontros pessoais, restaurantes / jantar, portais de busca, shopping e portais de compras, MP3, download de software, viagens e WEB hosting. Deve possuir capacidade de submissão instantânea de novos sites e palavras chaves. Deve permitir alterar localmente a classificação de algum site. Deve implementar a função de Proxy transparente internamente ou apontando para um servidor externo. Deve permitir priorizar e/ou limitar banda por categoria de filtro de conteúdo. A página de bloqueio do filtro de conteúdo deve ser totalmente customizada via HTML. Deve permitir integração com a base LDAP, de forma que seja possível implementar políticas de filtro de conteúdos diferenciados para grupos distintos de usuários. O administrador de política de segurança deve poder definir grupos de usuários e diferentes políticas de filtragem de sites WEB, personalizando quais categorias deverão ser bloqueadas ou permitidas para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet.
2	**Aquisição de uma nova solução de Firewall (hardware e licença) com suporte técnico e garantia do appliance em Par de Alta Disponibilidade e software de gerência de logs e relatórios centralizados, ambos pelo período de 24 meses.** Deve possuir pelo menos 4 interfaces 10Gbps. Deve possuir o Threat prevention throughput de pelo menos 15Gbps.

Deve possuir o IPsec VPN throughput de pelo menos 15Gbps.

Deve possuir Anti-malware inspection Throughput de pelo menos 15Gbps.

Deve possuir IPS Throughput de pelo menos 15Gbps.

Deve suportar conexões simultâneas de pelo menos 3.000.000 de usuários.

Deve permitir suporte a, no mínimo, 228.000 novas conexões por segundo.

Deve possuir Throughput de Inspeção de Aplicações de pelo menos 20Gbps.

Deve permitir suporte a, no mínimo, 6.000 Site-to-Site VPN Tunnels.

Deve permitir suporte a, no mínimo, 2000 IPSec VPN Clients.

Deve possuir suporte a SSL VPN.

Deve possuir no mínimo 512 interfaces VLAN.

A solução deve prover as seguintes funcionalidades:

IPS / Gateway AV / Controle de aplicações

IDS interno, capaz de detectar e evitar, automaticamente, IP Source Spoofing, IP Source Routing, Tunel IPsec e ataques tipo DoS (Denial-of-Service) como Ping of Death, SYN Flood, LAND Attack, IP Spoofing, com a possibilidade de se atualizar as assinaturas e carregar novas por meio da atualização do software de sistema operacional do equipamento (appliance).

Deve implementar assinaturas dinâmicas de IPS (Intrusion Prevention System) capaz de realizar inspeção no campo de "Dados" do pacote IP para detecção e prevenção de ataques.

A funcionalidade de IPS deve possuir no mínimo 3.500 (três mil e quinhentas) assinaturas contra ataques, carregadas automaticamente no equipamento quando ativado o serviço.

Deve implementar assinaturas dinâmicas de Gateway Antivírus capaz de realizar inspeção no campo de "Dados" do pacote IP para detecção e prevenção de virus, worms, spywares, malwares, etc.

A funcionalidade de Gateway Antivírus deve possuir no mínimo 20.000 (vinte mil) assinaturas contra ataques, carregadas automaticamente no equipamento quando ativado o serviço. Essa funcionalidade não deve possuir limitação de tamanho de arquivo para varredura.

Gateway Antivírus deve ser capaz de identificar ameaças nos seguintes protocolos: HTTP, SMTP, POP, IMAP, CIFS/NETBIOS e TCP STREAM.

Deve possuir flexibilidade para liberar aplicações da inspeção profunda de pacotes, ou seja, excluir a aplicação da checagem de IPS, Gateway Antivirus/AntiSpyware.

Deve possuir funcionalidade para bloquear, limitar e garantir banda baseada em assinaturas de aplicações. Deve possuir no mínimo 4.000 (quatro mil) assinaturas de aplicações, carregadas automaticamente no equipamento quando ativado o serviço.

Deve permitir a criação de assinaturas customizadas via interface gráfica de gerenciamento.

Deve permitir a restrição de arquivos por sua extensão e bloqueio de anexos por meio de protocolos SMTP e POP3 baseado em seus nomes ou tipos mime.

Deve permitir a filtragem de e-mails pelo seu conteúdo, por meio da definição de palavras-chave e a sua forma de pesquisa.

Filtro de conteúdo WEB

Deve implementar checagem de URLs requisitadas pelos usuários e classificá-las em categorias para que possam ser bloqueadas, liberadas e/ou ter a utilização de banda customizada. As consultas para categorizar as URLs deverão ser dinâmicas via Internet utilizando base de dados do mesmo ou de outro fabricante.

Deve possuir no mínimo 40 (quarenta) categorias de URL e com, pelo menos, as seguintes categorias: violência, nudismo, roupas intimas / banho, pornografia, armas, ódio / racismo, cultos / ocultismo, drogas / drogas ilegais, crimes / comportamento ilegal, educação sexual, jogos, álcool / tabagismo, conteúdo adulto, conteúdo questionável, artes e entretenimento, bancos / e trading, chat, negócios e economia, tecnologia de computadores e Internet, e-mail pessoal, jogos de azar, hacking, humor, busca de empregos, newsgroups, encontros pessoais, restaurantes / jantar, portais de busca, shopping e portais de compras, MP3, download de software, viagens e WEB hosting.

Deve possuir capacidade de submissão instantânea de novos sites e palavras chaves.

Deve permitir alterar localmente a classificação de algum site.

Deve implementar a função de Proxy transparente internamente ou apontando para um servidor externo.

Deve permitir priorizar e/ou limitar banda por categoria de filtro de conteúdo.

A página de bloqueio do filtro de conteúdo deve ser totalmente customizada via HTML.

Deve permitir integração com a base LDAP, de forma que seja possível implementar políticas de filtro de conteúdos diferenciados para grupos distintos de usuários.

O administrador de política de segurança deve poder definir grupos de usuários e diferentes políticas de filtragem de sites WEB, personalizando quais categorias deverão ser bloqueadas ou permitidas para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet.

Software de Gerência de Logs e Relatórios Centralizados

Deve possuir solução de logs e relatórios centralizados, possibilitando a consolidação total de todas as atividades da solução por meio de uma única console central.

Deve estar licenciada para gerenciar as soluções de firewall de próxima geração.

Devem ser fornecidas soluções virtuais ou via appliances desde que obedeçam a todos os requisitos desta especificação, com armazenamento mínimo de 1TB de dados.

Deve prover relatórios baseados em usuários, com visibilidade sobre acesso a aplicações, navegação, eventos ATP, downloads e consumo de banda, independente em qual rede ou IP o usuário esteja se conectando.

Deve possibilitar a identificação de ataques como a identificação de malware identificados pelos eventos ATP, usuários suspeitos, tráfegos anômalos incluindo tráfego ICMP e consumo não-usual de banda.

	Deve conter relatórios pré-configurados, pelo menos de: aplicações, navegação, web server (WAF), IPS, ATP e VPN. Deve fornecer relatórios históricos para análises de mudanças e comportamentos. Deve conter customizações dos relatórios para inserção de logotipos próprios. Deve fornecer relatórios de compliance SOX, HIPAA e PCI. Deve permitir a exportação via PDF ou Excel. Deve fornecer relatórios sobre os acessos de procura no Google, Yahoo, Bing e Wikipedia. Deve fornecer relatórios de tendências. Deve fornecer logs em tempo real, de auditoria e arquivados. Deve possuir mecanismo de procura de logs arquivados. Deve ter acesso baseado em Web com controles administrativos distintos.
3	**Atualização do Firewall SonicWall Supermassive 9600 para o NSA 5700 e aquisição da licença Essential Protection Service Suite for NSA 5700 em Par de Alta Disponibilidade e licença adicional SonicWall Analytics Software for NSA 5700, ambos pelo período de 24 meses.** Deve possuir pelo menos 4 interfaces 10Gbps. Deve possuir o Threat prevention throughput de pelo menos 15Gbps. Deve possuir o IPsec VPN throughput de pelo menos 15Gbps. Deve possuir Anti-malware inspection Throughput de pelo menos 15Gbps. Deve possuir IPS Throughput de pelo menos 15Gbps. Deve suportar conexões simultâneas de pelo menos 3.000.000 de usuários. Deve permitir suporte a, no mínimo, 228.000 novas conexões por segundo. Deve possuir Throughput de Inspeção de Aplicações de pelo menos 20Gbps. Deve permitir suporte a, no mínimo, 6.000 Site-to-Site VPN Tunnels. Deve possuir suporte a, no mínimo, 2000 IPSec VPN Clients. Deve possuir suporte a SSL VPN. Deve possuir no mínimo 512 interfaces VLAN. A solução deve prover as seguintes funcionalidades: **IPS / Gateway AV / Controle de aplicações**

IDS interno, capaz de detectar e evitar, automaticamente, IP Source Spoofing, IP Source Routing, Tunel IPsec e ataques tipo DoS (Denial-of-Service) como Ping of Death, SYN Flood, LAND Attack, IP Spoofing, com a possibilidade de se atualizar as assinaturas e carregar novas por meio da atualização do software de sistema operacional do equipamento (appliance).

Deve implementar assinaturas dinâmicas de IPS (Intrusion Prevention System) capaz de realizar inspeção no campo de "Dados" do pacote IP para detecção e prevenção de ataques.

A funcionalidade de IPS deve possuir no mínimo 3.500 (três mil e quinhentas) assinaturas contra ataques, carregadas automaticamente no equipamento quando ativado o serviço.

Deve implementar assinaturas dinâmicas de Gateway Antivírus capaz de realizar inspeção no campo de "Dados" do pacote IP para detecção e prevenção de virus, worms, spywares, malwares, etc.

A funcionalidade de Gateway Antivírus deve possuir no mínimo 20.000 (vinte mil) assinaturas contra ataques, carregadas automaticamente no equipamento quando ativado o serviço. Essa funcionalidade não deve possuir limitação de tamanho de arquivo para varredura.

Gateway Antivírus deve ser capaz de identificar ameaças nos seguintes protocolos: HTTP, SMTP, POP, IMAP, CIFS/NETBIOS e TCP STREAM.

Deve possuir flexibilidade para liberar aplicações da inspeção profunda de pacotes, ou seja, excluir a aplicação da checagem de IPS, Gateway Antivirus/AntiSpyware.

Deve possuir funcionalidade para bloquear, limitar e garantir banda baseada em assinaturas de aplicações. Deve possuir no mínimo 4.000 (quatro mil) assinaturas de aplicações, carregadas automaticamente no equipamento quando ativado o serviço.

Deve permitir a criação de assinaturas customizadas via interface gráfica de gerenciamento.

Deve permitir a restrição de arquivos por sua extensão e bloqueio de anexos por meio de protocolos SMTP e POP3 baseado em seus nomes ou tipos mime.

Deve permitir a filtragem de e-mails pelo seu conteúdo, por meio da definição de palavras-chave e a sua forma de pesquisa.

Filtro de conteúdo WEB

Deve implementar checagem de URLs requisitadas pelos usuários e classificá-las em categorias para que possam ser bloqueadas, liberadas e/ou ter a utilização de banda customizada. As consultas para categorizar as URLs deverão ser dinâmicas via Internet utilizando base de dados do mesmo ou de outro fabricante.

Deve possuir no mínimo 40 (quarenta) categorias de URL e com, pelo menos, as seguintes categorias: violência, nudismo, roupas intimas / banho, pornografia, armas, ódio / racismo, cultos / ocultismo, drogas / drogas ilegais, crimes / comportamento ilegal, educação sexual, jogos, álcool / tabagismo, conteúdo adulto, conteúdo questionável, artes e entretenimento, bancos / e trading, chat, negócios e economia, tecnologia de computadores e Internet, e-mail pessoal, jogos de azar, hacking, humor, busca de empregos, newsgroups, encontros pessoais, restaurantes / jantar, portais de busca, shopping e portais de compras, MP3, download de software, viagens e WEB hosting.

Deve possuir capacidade de submissão instantânea de novos sites e palavras chaves.

Deve permitir alterar localmente a classificação de algum site.

Deve implementar a função de Proxy transparente internamente ou apontando para um servidor externo.

	Deve permitir priorizar e/ou limitar banda por categoria de filtro de conteúdo. A página de bloqueio do filtro de conteúdo deve ser totalmente customizada via HTML. Deve permitir integração com a base LDAP, de forma que seja possível implementar políticas de filtro de conteúdo diferenciados para grupos distintos de usuários. O administrador de política de segurança deve poder definir grupos de usuários e diferentes políticas de filtragem de sites WEB, personalizando quais categorias deverão ser bloqueadas ou permitidas para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

1	Suporte técnico 24x7, por parte do fabricante: o suporte técnico deve ser disponibilizado durante 24 horas, 7 dias por semana. Esse suporte é essencial em caso de sinistro com o equipamento.
2	Suporte técnico 8x5, por parte da Contratada: o suporte técnico deve ser disponibilizado durante 8 horas, 5 dias por semana. Esse suporte deve ser ilimitado, com plantão de emergência, treinamento ilimitado, monitoramento, backup diário e relatórios de service desk.

7. Estimativa da demanda - quantidade de bens e serviços

A Universidade Federal de Lavras disponibiliza uma infraestrutura de TI para cerca de 20.000 (vinte mil) usuários da comunidade acadêmica, sendo composta por alunos, professores e técnicos administrativos em educação.

Atualmente, possui a solução da SonicWall Supermassive 9600, que permite um nível de segurança na filtragem de pacotes, aplicando regras de bloqueios nas camadas de rede e transporte do modelo OSI, Filtro de Botnet, Gateway (Antivírus, Anti-Spyware, Prevenção de Intrusão) filtro de conteúdo, possibilidade de atualização de software e firmware, alta disponibilidade, gerenciamento centralizado das configurações, alertas e logs.

Outro fator que deve ser ressaltado é a ausência de mecanismos que permitam o monitoramento do tráfego. Nesse contexto, os gestores da rede não conseguem obter uma visão mais detalhada do tráfego a nível das aplicações que estão trafegando dados, qual o nível de risco do tráfego e se ele pode trazer ameaças para a rede. Esse tipo de informação é muito importante para prover uma rápida análise caso ocorra algum incidente e para a geração de relatórios sobre uso da banda, o que auxilia a diagnosticar de forma rápida e eficiente as causas de possíveis ataques cibernéticos ou lentidão na rede.

Porém, o equipamento possui mais de seis anos de uso, onde as licenças dos softwares internos vencerão em Junho de 2022, deixando a universidade vulnerável a ataques externos. Para que isso não ocorra, faz-se necessária a renovação das licenças dos softwares internos do firewall nos seguintes quantitativos:

Descrição	Quantidade	Tempo da licen
Contratação de solução de Firewall, implantação, garantia e suporte técnico.	1	2 anos
Contratação de software de gerência de Logs e relatórios centralizados, implantação, garantia e suporte técnico.	1	2 anos

Todavia, com o crescimento, na UFLA, da infraestrutura computacional e as novas demandas surgindo devido às novas tecnologias emergentes, o atual firewall está quase atingindo sua capacidade máxima de gerir as informações na rede da UFLA. Uma atualização do equipamento, futuramente, com, no mínimo, as mesmas funcionalidades de hoje em dia, é necessária, porém, com uma maior capacidade de recursos para abarcar o crescimento futuro da instituição e as novas demandas que surgirem.

8. Levantamento de soluções

Este estudo tem como objetivo indicar o melhor cenário para a atualização e ampliação do firewall da UFLA. Para isso, foram identificados três possíveis cenários viáveis:

8.1 - Solução 1 - Atualização das licenças e Analytics.

Essa solução se baseia em apenas atualizar as licenças e adquirir o Analytics como software de análise dos logs.

- Aquisição da licença Advanced Gateway Security Suite (AGSS);
- Licença adicional SonicWall Analytics Software;
- Renovação do suporte técnico;
- Garantia do appliance de firewall SonicWall Supermassive 9600 em par de alta disponibilidade.

8.2 - Solução 2 - Aquisição de uma nova solução de Firewall.

Essa solução se baseia na compra de uma nova appliance Next-Generation (NGFW) para substituir o firewall. Essa alternativa visa contemplar possível solução de outro fabricante que possa vir a atender os requisitos necessários à UFLA.

8.3 - Solução 3 - Upgrade do hardware, atualização das licenças e contratação do SonicWall Analytics.

Esse cenário de solução visa estudar a troca do hardware existente por equipamento superior da mesma fabricante, atualizar a licença do software e a aquisição da licença do SonicWall Analytics.

Id	Descrição da solução (ou cenário)
1	Renovação da licença Advanced Gateway Security Suite (AGSS) com suporte técnico e garantia do appliance em Par de Alta Disponibilidade por 24 meses, com serviço mensal de Service Desk prestado pelo fornecedor em regime de 8/5, pelo período de 12 meses + aquisição da licença SonicWall Analytics Software pelo período de 24 meses.
2	Aquisição de uma nova solução de Firewall (hardware e licença) com suporte técnico e garantia do appliance em Par de Alta Disponibilidade por 24 meses, com migração do Supermassive 9600 para a nova solução + licença software de Gerência de Logs e Relatórios Centralizados pelo período de 24 meses.

3	Atualização do Firewall SonicWall Supermassive 9600 para o NSA 5700 e aquisição da licença Essential Protection Service Suite para NSA 5700 em Par de Alta Disponibilidade por 24 meses, com serviço mensal de Service Desk prestado pelo fornecedor em regime de 8/5, pelo período de 12 meses + aquisição da licença SonicWall Analytics Software pelo período de 24 meses.

9. Análise comparativa de soluções

A solução 1 (renovação da licença): prevê a renovação da licença do atual appliance SonicWall Supermassive 9600 utilizado pela Instituição, com a compra de uma licença Advanced Gateway Security Suite (AGSS) + licença adicional SonicWall Analytics Software, pelo período de 24 meses. Com as constantes mudanças na quantidade de máquinas do parque tecnológico da Instituição e no crescente número de novos usuários, essa renovação apenas do licenciamento do equipamento existente não contempla o necessário aumento da capacidade de processamento do atual equipamento, o que pode resultar em gargalos e lentidão na rede. O atual appliance já possui cerca de 6 anos de uso e seu poder de processamento e suas soluções de defesa e segurança encontram-se, atualmente, deficientes em relação aos atuais Next-Generation Firewall (NGFW). Essa solução considera apenas a manutenção do hardware existente, não implicando em melhorias na disponibilidade de rede e segurança de dados institucionais. O prazo de renovação estudado foi de 24 (vinte e quatro) meses.

A solução 2 (aquisição de novo hardware + licenças necessárias): prevê a compra de uma nova solução de Next-Generation Firewall (NGFW), que prevê novas funcionalidades e maior poder de processamento em relação ao atual equipamento, como a proteção de informação perimetral e de rede interna, que inclui stateful firewall com capacidade para controle de tráfego de dados por identificação de usuários e por camada 7, com controle de aplicação, administração de largura de banda (QoS), VPN IPsec e SSL, IPS, prevenção contra ameaças de vírus, malwares, Filtro de URL, criptografia de email, inspeção de tráfego criptografado e proteção de firewall de aplicação Web. Algumas dessas funcionalidades, que agregam uma maior proteção aos ativos de informação da Instituição, não são contempladas, atualmente, pelo firewall utilizado pela Instituição. A compra de um novo equipamento de firewall (hardware) proporcionará maior robustez à segurança da rede e do gerenciamento das conexões estabelecidas na UFLA. O equipamento comparado nessa solução se trata de solução tão atualizada e robusta quanto a solução analisada na Solução 03 (Upgrade do Hardware SonicWall, atualização das licenças e contratação do SonicWall Analytics). Ou seja, nas Soluções 02 e 03, os equipamentos terão maior disponibilidade de atendimento, considerando o crescimento orgânico da Universidade.

A solução 3 (upgrade do hardware SonicWall + renovação da licença): prevê a atualização da solução de firewall já existente na Instituição, ou seja, aquisição de novo hardware da mesma fabricante, já utilizado pela UFLA (por exemplo o modelo SonicWall NSA 5700). Essa modalidade possibilita ganhos financeiros com eventuais descontos para se fazer o “upgrade” do hardware. A compra de um novo equipamento de firewall (hardware) proporcionará maior robustez à segurança da rede e do gerenciamento das conexões estabelecidas na UFLA. Por meio da Solução 03 será possível à UFLA manter a continuidade da prestação de serviços, ao considerar a manutenção da mesma marca de equipamento e treinamento de equipe. E ainda, com o upgrade do hardware, a instituição obterá maior disponibilidade de rede, melhoria na taxa de uplink da rede.

Requisito	Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
	Solução 2	X		
	Solução 3	X		

A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1		X	
	Solução 2		X	
	Solução 3		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			X
	Solução 3			X

Ademais, foi verificado por parte da equipe técnica que o dispêndio financeiro para aquisição de novo firewall seria gravoso à universidade, por demandar recursos de capital, no atual cenário orçamentário. Assim, a aquisição de novo firewall pode ser objeto de análise em novo PAC/PDTIC. Para o momento, o equipamento patrimoniado pela UFLA atende plenamente às necessidades institucionais.

A Equipe de Planejamento da Contratação ressalta que a inclusão de novas tecnologias e demandas digitais podem interferir na usabilidade do equipamento atual e gerar a necessidade de troca do mesmo. No entanto, esse não é o cenário atual, configurando uma possibilidade futura e que será tratada na matriz de risco da contratação.

10. Registro de soluções consideradas inviáveis

O levantamento e a análise comparativa de soluções consideraram apenas as soluções viáveis, conforme observado nos itens 8 e 9, acima. Como soluções inviáveis, foram identificadas:

Não renovar a licença - Não realizar a renovação do licenciamento da solução atual e utilizar o equipamento sem garantia e com funções limitadas levaria a desativação de funções importantes, expondo a UFLA e seus usuários a um ambiente inseguro.

Software Livre - Não existe um único produto baseado em software livre que seja capaz de oferecer todas as funcionalidades oferecidas por outros softwares proprietários reunidas em um único produto. Para implementação da solução por meio de software livre, seria necessário utilizar várias soluções diferentes e não integradas, tais como Firewall Iptables, Web Filter Squid, OpenVPN e IPS Snort etc., aumentando exponencialmente o esforço de implementação e sustentação, falta de garantia em caso de falhas no software e ausência de suporte. Além disso, deve ser considerada a curva de aprendizagem, com capacitação e especialização do corpo técnico existente nas diversas soluções open sources citadas e o possível custo de contratação de mão de obra especializada, tempo para implementação e custos indiretos.

Contratação de solução de firewall na modalidade de serviço - Por se tratar de uma solução com contratação na modalidade de serviço, a qual depende de pagamentos mensais para a continuidade na prestação de serviço, tal contratação depende da disponibilidade de verbas destinadas a custeio. A inclusão de mais uma despesa mensal na já escassa verba de custeio traria ainda mais problemas para a administração do orçamento.

11. Análise comparativa de custos (TCO)

Cálculo dos Custos Totais de Propriedade

O cálculo dos Custos Totais de Propriedade, incluindo os dados e as memórias de cálculo para cada solução, encontram-se no Anexo I deste Estudo Técnico Preliminar (Pesquisa de Preços.pdf).

Solução Viável 1 - Renovação da Assinatura e Contratação do Analytics

Descrição:

Aquisição da licença Advanced Gateway Security Suite (AGSS) e licença adicional SonicWall Analytics Software renovação do suporte técnico e garantia do appliance de firewall SonicWall Supermassive 9600 em Par de Disponibilidade pelo período de 24 meses.

Custo Total de Propriedade – Memória de Cálculo

Item	Descrição	Quant.	Valor Unitário Estimado	Valor Total Estimado
1		1	R$ 479.359,77	R$ 479.359,77

	Renovação da licença Advanced Gateway Security Suite (AGSS) com suporte técnico e garantia do appliance em Par de Alta Disponibilidade por 24 meses, com serviço mensal de Service Desk prestado pelo fornecedor em regime de 8/5, pelo período de 12 meses.			
2	Aquisição da licença SonicWall Analytics Software pelo período de 24 meses.	1	R$ 19.407,91	R$ 19.407,91
Total Estimado Geral				**R$ 498.767,68**

Solução Viável 2 - Aquisição de Nova Solução de Hardware + Licenças Necessárias

Descrição:

Aquisição de uma nova solução de Firewall (hardware e licença) com suporte técnico e garantia do appliance em Par de Alta Disponibilidade pelo período de 24 meses.

Custo Total de Propriedade – Memória de Cálculo

Item	Descrição	Quantidade	Valor Unitário Estimado	Valor Total Estimado
1	Aquisição de uma nova solução de Firewall (hardware e licença) com suporte técnico e garantia do appliance em Par de Alta Disponibilidade por 24 meses, com migração do Supermassive 9600 para a nova solução.	1	R$ 1.135.942,07	R$ 1.135.942,07
2	Licença software de Gerência de Logs e Relatórios Centralizados pelo período de 24 meses.	1	R$ 74.156,46	R$ 74.156,46
Total Estimado Geral				**R$ 1.210.098,53**

Solução Viável 3 - Upgrade do Hardware SonicWall + Renovação da Licença

Descrição:

Atualização do antigo Firewall SonicWall (troca do hardware) e renovação da licença.

Custo Total de Propriedade – Memória de Cálculo

Item	Descrição	Quant.	Valor Unitário Estimado	Valor Total Estimado
1	Atualização do Firewall SonicWall Supermassive 9600 para o NSA 5700 e aquisição da licença Essential Protection Service Suite para NSA 5700 em Par de Alta Disponibilidade por 24 meses, com migração do Supermassive 9600 para a nova solução, com serviço mensal de Service Desk prestado pelo fornecedor em regime de 8/5, pelo período de 12 meses.	1	R$ 452.484,47	R$ 452.484,47
2	Aquisição da licença SonicWall Analytics Software pelo período de 24 meses.	1	R$ 9.022,19	R$ 9.022,19
Total Estimado Geral				**R$ 461.506,66**

Mapa Comparativo dos Cálculos Totais de Propriedade (TCO)

Descrição da solução	Estimativa de TCO ao longo dos anos			Total
	2022	2023	2024	
Solução 1 - Renovação da Assinatura e Contratação do Analytics.	**R$ 498.767,68**	-	-	**R$ 498.767,68**

Solução 2 - Aquisição de Hardware + Licenças Necessárias e Contratação do Analytics.	**R$ 1.210.098,53**	**-**	**-**	**R$ 1.210.098,53**
Solução 3 - Upgrade do Hardware SonicWall + Renovação da Licença e Contratação do Analytics.	**R$ 461.506,66**	**-**	**-**	**R$ 461.506,66**

12. Descrição da solução de TIC a ser contratada

Cenário	Descrição
Solução 3	Atualização do Firewall SonicWall Supermassive 9600 para o NSA 5700 e aquisição da licença Essential Protection Service Suite para NSA 5700 em Par de Alta Disponibilidade por 24 meses, com serviço mensal de Service Desk prestado pelo fornecedor em regime de 8/5, pelo período de 12 meses. E aquisição da licença SonicWall Analytics Software pelo período de 24 meses.

13. Estimativa de custo total da contratação

Valor (R$): 461.506,66

Serviço	Estimativa
Atualização do Firewall SonicWall Supermassive 9600 para o NSA 5700 e aquisição da licença Essential Protection Service Suite para NSA 5700 em Par de Alta Disponibilidade por 24 meses, com serviço mensal de Service Desk prestado pelo fornecedor em regime de 8/5, pelo período de 12 meses.	1 unidade x R$ 452.484,47
Total do Item:	R$ 452.484,47
Aquisição da licença SonicWall Analytics Software pelo período de 24 meses.	1 unidade x R$ R$ 9.022,19
Total do Item:	R$ R$ 9.022,19
Estimativa de Custo Total da Contratação	
R$ 461.506,66	

14. Justificativa técnica da escolha da solução

Considera-se tecnicamente viável a Solução 03 pela necessidade de um novo equipamento para atender as demandas de expansão da rede ocorridas nos últimos anos, desde a compra do último equipamento, e contemplar as futuras expansões nos próximos anos. O modelo de firewall usado atualmente possui deficiências de capacidade de processamento que impedem o uso de módulos essenciais para a segurança da rede, como a inspeção profunda de pacotes de dados SSL, o controle de Flood de pacotes na rede, que permite a contenção no caso de ataques.

É importante observar o aumento da demanda de uso da banda de Internet existente na UFLA. Isso se deve ao fato de que, com o passar dos anos, a infraestrutura de TI da Universidade cresceu muito, com a disseminação da Internet móvel, permitindo a proliferação dos dispositivos pessoais dentro dessa infraestrutura e, considerando a evolução das aplicações e métodos de criptografia SSL utilizados na maioria das conexões existentes, acarretou em extrema complexidade para a gestão da segurança da informação. Esse aspecto torna-se mais importante em um cenário de expansão de link, onde a solução de firewall atual não suportaria um aumento na banda disponível ou a implementação de novos mecanismos de segurança, pois, atualmente, a solução em questão já trabalha com o máximo da sua capacidade.

Além de oferecer um nível maior de segurança à rede, um firewall de próxima geração, com uma maior capacidade de processamento, possibilita a implementação de novos serviços, como por exemplo, análise do tráfego. Com isso, seria possível ter uma visualização detalhada da utilização da rede e das aplicações utilizadas. Adicionalmente, o processo de identificação de ameaças é facilitado e permite a aplicação de políticas de segurança mais eficientes. Outra funcionalidade importante que pode ser implementada é a identificação de usuários que utilizam a rede e o registro de conexões, permitindo um melhor inventário dos ativos de TI da UFLA.

Com o aumento no número de usuários trabalhando de casa, a quantidade de conexões externas para trabalho home office aumentou consideravelmente durante o período de pandemia, aumentando a necessidade de conexões VPN suportadas pelo equipamento antigo. O aumento na quantidade de ataques às empresas, durante a pandemia, principalmente na tentativa de sequestro de dados em troca de resgate, fez com que a necessidade de um firewall que pudesse conter ataques de negação de serviço e bloquear infecções maliciosas, principalmente em casos de ataques de ransomware, aumentasse a necessidade de um equipamento capaz de comportar uma maior e mais rápida análise do tráfego de dados na rede institucional.

15. Justificativa econômica da escolha da solução

Levando em consideração o crescimento da rede da universidade nos últimos cinco anos, será preciso um maior poder de processamento para lidar com tráfego diário na rede. Por esse motivo, a Solução 03 se mostra de acordo com esse objetivo, que será aumentar o poder de processamento e throughput, sem a necessidade de grandes incrementos de despesa.

Por exemplo, o Firewall atual conta com 20Gb de Firewall throughput, enquanto o novo aparelho disponibilizará 36Gb nesse mesmo item de especificação. Assim, a manutenção do firewall atual custa em torno de R$21.895,00 por GB disponível, e a nova solução tem como custo R$16.552,19 por GB disponível, uma economia de mais de 30% em termos de disponibilidade X custo.

A Solução 03 se torna mais barata, pois nela está incluso um ganho de escala pela manutenção do software (que não implica em custos adversos) e pela melhoria em termos de tecnologia, ao se adquirir um aparelho de nova geração.

Ademais, o upgrade do firewall do mesmo fabricante proporciona vantagem à UFLA, por ser possível obter desconto na aquisição de um aparelho novo da mesma marca e ainda proporcionar a competitividade dos concorrentes fornecedores dos produtos SonicWall.

16. Benefícios a serem alcançados com a contratação

Aumentar a disponibilidade dos sistemas institucionais por meio de uma melhor e mais segura infraestrutura de redes, melhorando a continuidade dos processos de negócio.

Aumentar a velocidade de acesso à Internet, para usuários institucionais, aproveitando toda a largura de banda disponibilizada para a Universidade.

Melhorar a capacidade de bloqueio de ataques e conexões estranhas aos serviços de tecnologia da informação da UFLA, tendo uma maior e mais precisa visibilidade do tráfego que passa pelo firewall, podendo analisar melhor possíveis ameaças, identificando problemas na rede e salvaguardando seus ativos de tecnologia da informação, criando um isolamento seguro dos serviços de tecnologia.

17. Providências a serem Adotadas

Em termos de providências a serem tomadas, a equipe técnica considera ser relevante realizar as seguintes ações: divulgar amplamente à comunidade acadêmica acerca das datas de migração dos aparelhos, verificação de disponibilidade de servidores nos dias de instalação, acompanhamento e gestão adequada do contrato.

18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

18.1. Justificativa da Viabilidade

A solução viável definida como a eleita para contratação - Solução 03 - foi assim considerada por contemplar, tecnicamente e economicamente, as necessidades atuais definidas pela instituição, conforme exposto ao longo deste Estudo Técnico Preliminar. Assim conforme mencionado acima, a Solução 03 proporcionará, em resumo:

- Atualização da licença de Software já utilizada;
- Melhoria de Hardware;
- Maior qualidade na análise de dados trafegados na rede;
- Maior disponibilidade de rede;
- Maior segurança de TI.

19. Responsáveis

PLÍNIO MÁRCIO BRAGA TORRES

Integrante Requisitante

JAIRO ANTÔNIO RESENDE PAVIANI

Integrante Técnico

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - 000 Pesquisas de Preços nova.pdf (7.74 MB)

Anexo I - 000 Pesquisas de Preços nova.pdf

UNIVERSIDADE FEDERAL DE LAVRAS
REITORIA
SUPERINTENDÊNCIA DE GOVERNANÇA
DIRETORIA DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO
COORDENADORIA DE AQUISIÇÕES DE TECNOLOGIA DA INFORMAÇÃO

Lavras, 12 de julho de 2022.

PESQUISA DE PREÇOS

Na condição de integrante técnico da equipe de planejamento da contratação, instaurada pela Portaria SGV/Reitoria nº 09, de 08 de março de 2022, reconduzida pela Portaria SGV/Reitoria nº 19, de 13 de maio de 2022, tendo em vista a Pesquisa de Preços, nessa fase do processo de contratação, venho apresentar os valores estimados para a contratação de empresa especializada no fornecimento de solução de segurança da informação (Firewall).

Tabela de Quantitativos para Pesquisa de Preços

Descrição	Quantidade	Tempo da licença
Contratação de solução de Firewall, implantação, garantia e suporte técnico.	1	2 anos
Contratação de software de gerência de Logs e relatórios centralizados, implantação, garantia e suporte técnico.	1	2 anos

A pesquisa foi realizada considerando três cenários de soluções viáveis, que se diferenciavam pelo tipo de aquisição a ser feita, por meio da atualização apenas da licença existente ou da compra de um novo hardware ou atualização do hardware existente:

Solução Viável 01 - Renovação da licença com suporte técnico e garantia do firewall SonicWall Supermassive 9600 e aquisição da licença SonicWall Analytics Software, ambas pelo período de 24 meses;

Solução Viável 02 - Aquisição de uma nova solução de Firewall (hardware e licença) com suporte técnico e garantia e aquisição da licença de um software de Gerência de Logs e Relatórios Centralizados, ambas pelo período de 24 meses;

Solução Viável 03 - Atualização do Firewall SonicWall Supermassive 9600 para uma hardware de maior capacidade e com suporte técnico e garantia e licença adicional SonicWall Analytics Software, ambas pelo período de 24 meses.

A **Solução 03** foi considerada a mais viável, com os itens nas quantidades supracitadas, não presentes nos Catálogos de Soluções de TIC com Condições Padronizadas, publicados pela Secretaria de Governo Digital da Secretaria Especial de Desburocratização, Gestão e Governo Digital, resultando nos seguintes valores estimados:

UNIVERSIDADE FEDERAL DE LAVRAS
REITORIA
SUPERINTENDÊNCIA DE GOVERNANÇA
DIRETORIA DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO
COORDENADORIA DE AQUISIÇÕES DE TECNOLOGIA DA INFORMAÇÃO

Tabela de Valores Estimados da Pesquisa de Preço para a Solução Viável 03

Item	Descrição	Quant.	Valor Unitário Estimado	Valor Total Estimado
1	Atualização do Firewall SonicWall Supermassive 9600 para o NSA 5700 e aquisição da licença Essential Protection Service Suite para NSA 5700 em Par de Alta Disponibilidade por 24 meses, com migração do Supermassive 9600 para a nova solução, com serviço mensal de Service Desk prestado pelo fornecedor em regime de 8/5, pelo período de 12 meses.	1	R$ 452.484,47	R$ 452.484,47
2	Aquisição da licença SonicWall Analytics Software pelo período de 24 meses.	1	R$ 9.022,19	R$ 9.022,19
			Total Estimado Geral	**R$ 461.506,66**

Para comprovar esse resultado, seguem em anexo:

Tabela de Valores Estimados da Pesquisa de Preço para a Solução Viável 01;
Tabela de Cálculo do valor estimado para o item 1 da Solução 01;
Tabela de Cálculo do valor estimado para o item 2 da Solução 01;
Tabela de Valores Estimados da Pesquisa de Preço para a Solução Viável 02;
Tabela de Cálculo do valor estimado para o item 1 da Solução 02;
Tabela de Cálculo do valor estimado para o item 2 da Solução 02;
Tabela de Valores Estimados da Pesquisa de Preço para a Solução Viável 03;
Tabela de Cálculo do valor estimado para o item 1 da Solução 03;
Tabela de Cálculo do valor estimado para o item 2 da Solução 03.

_____
JAIRO ANTONIO RESENDE PAVIANI
Integrante Técnico

UNIVERSIDADE FEDERAL DE LAVRAS
REITORIA
SUPERINTENDÊNCIA DE GOVERNANÇA
DIRETORIA DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO
COORDENADORIA DE AQUISIÇÕES DE TECNOLOGIA DA INFORMAÇÃO

Tabela de Valores Estimados da Pesquisa de Preço para a Solução Viável 01

Item	Descrição	Quant.	Valor Unitário Estimado	Valor Total Estimado
1	Renovação da licença Advanced Gateway Security Suite (AGSS) com suporte técnico e garantia do appliance em Par de Alta Disponibilidade por 24 meses, com serviço mensal de Service Desk prestado pelo fornecedor em regime de 8/5, pelo período de 12 meses.	1	R$ 479.359,77	R$ 479.359,77
2	Aquisição da licença SonicWall Analytics Software pelo período de 24 meses.	1	R$ 19.407,91	R$ 19.407,91
Total Estimado Geral				**R$ 498.767,68**

UNIVERSIDADE FEDERAL DE LAVRAS
REITORIA
SUPERINTENDÊNCIA DE GOVERNANÇA
DIRETORIA DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO
COORDENADORIA DE AQUISIÇÕES DE TECNOLOGIA DA INFORMAÇÃO

Tabela de Cálculo do valor estimado para o item 1 da Solução 01

ID	**Pesquisa de Preços -** Renovação da licença Advanced Gateway Security Suite (AGSS) com suporte técnico e garantia do appliance em Par de Alta Disponibilidade por 24 meses, com serviço mensal de Service Desk prestado pelo fornecedor em regime de 8/5, pelo período de 12 meses.	**DESCRIÇÃO / VALOR**	
1	Razão Social do Fornecedor: NETSOL LTDA CNPJ/CPF: 03.675.909/0001-38 Data: 03/06/2022	Advanced Gateway Security Suite Bundle for Supermassive 9600 2yr	R$ 387.073,83
		Service Desk prestado pelo fornecedor em regime de 8/5, pelo período de 12 meses.	R$ 43,344,00
		Total	**R$ 430.417,83**
2	Razão Social do Fornecedor: I.M. TECNOLOGIA E SISTEMAS EIRELI CNPJ/CPF: 08.042.908/0001-70 Data: 10/05/2022	Advanced Gateway Security Suite Bundle for Supermassive 9600 2yr	R$ 445.919,17
		Service Desk prestado pelo fornecedor em regime de 8/5, pelo período de 12 meses.	R$ 57.600,00
		Total	**R$ 503.519,17**
3	Razão Social do Fornecedor: MGSOFT COMÉRCIO E SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO LTDA CNPJ/CPF: 09.493.777.0001-00 Data: 10/05/2022	Advanced Gateway Security Suite Bundle for Supermassive 9600 2yr	R$ 453.742,31
		Service Desk prestado pelo fornecedor em regime de 8/5, pelo período de 12 meses.	R$ 50.400,00
		Total	**R$ 504.142,31**
Valor Unitário Estimado para o Item 1 (Média)		**R$ 479.359,77**	

UNIVERSIDADE FEDERAL DE LAVRAS
REITORIA
SUPERINTENDÊNCIA DE GOVERNANÇA
DIRETORIA DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO
COORDENADORIA DE AQUISIÇÕES DE TECNOLOGIA DA INFORMAÇÃO

Tabela de Cálculo do valor estimado para o item 2 da Solução 01

ID	**Pesquisa de Preços -** Aquisição da licença SonicWall Analytics Software pelo período de 24 meses.	**DESCRIÇÃO / VALOR**	
1	Razão Social do Fornecedor: NETSOL LTDA CNPJ/CPF: 03.675.909/0001-38 Data: 03/06/2022	SonicWall analytics software NSA9600 series pelo período de 24 meses.	R$ 17.514,78
2	Razão Social do Fornecedor: I.M. TECNOLOGIA E SISTEMAS EIRELI CNPJ/CPF: 08.042.908/0001-70 Data: 10/05/2022	SonicWall analytics software NSA9600 series pelo período de 24 meses.	R$ 20.177,48
3	Razão Social do Fornecedor: MGSOFT COMÉRCIO E SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO LTDA CNPJ/CPF: 09.493.777.0001-00 Data: 10/05/2022	SonicWall analytics software NSA9600 series pelo período de 24 meses.	R$ 20.531,47
Valor Unitário Estimado para o Item 2 (Média)		**R$ 19.407,91**	

UNIVERSIDADE FEDERAL DE LAVRAS
REITORIA
SUPERINTENDÊNCIA DE GOVERNANÇA
DIRETORIA DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO
COORDENADORIA DE AQUISIÇÕES DE TECNOLOGIA DA INFORMAÇÃO

Tabela de Valores Estimados da Pesquisa de Preço para a Solução Viável 02

Item	Descrição	Quant.	Valor Unitário Estimado	Valor Total Estimado
1	Aquisição de uma nova solução de Firewall (hardware e licença) com suporte técnico e garantia do appliance em Par de Alta Disponibilidade por 24 meses, com migração do Supermassive 9600 para a nova solução.	1	R$ 1.135.942,07	R$ 1.135.942,07
2	Licença software de Gerência de Logs e Relatórios Centralizados pelo período de 24 meses.	1	R$ 74.156,46	R$ 74.156,46
Total Estimado Geral				**R$ 1.210.098,53**

UNIVERSIDADE FEDERAL DE LAVRAS
REITORIA
SUPERINTENDÊNCIA DE GOVERNANÇA
DIRETORIA DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO
COORDENADORIA DE AQUISIÇÕES DE TECNOLOGIA DA INFORMAÇÃO

Tabela de Cálculo do valor estimado para o item 1 da Solução 02

ID	**Pesquisa de Preços -** Aquisição de uma nova solução de Firewall (hardware e licença) com suporte técnico e garantia do appliance em Par de Alta Disponibilidade por 24 meses, com migração do Supermassive 9600 para a nova solução.	**DESCRIÇÃO / VALOR**	
1	Razão Social do Fornecedor: NETSOL LTDA CNPJ/CPF: 03.675.909/0001-38 Data: 03/06/2022	02-SSC-4332 SONICWALL NSA 6700 - Sem Sec. Upgrade	R$ 294.179,59
		02-SSC-8988 SONICWALL NSA 6700 HIGH AVAILABILITY - Sem Sec. Upgrade	R$ 205.882,37
		02-SSC-9296 Licença ESSENTIAL PROTECTION SERVICE SUITE FOR NSA 6700 2YR	R$ 196.318,13
		Migração do Supermassive 9600 para o NSA5700.	R$ 8.342,00
		Total	**R$ 704.722,09**
2	Razão Social do Fornecedor: IT ONE TECNOLOGIA DA INFORMAÇÃO S.A. CNPJ/CPF: 05.333.907/0001-96 Data: 02/06/2022	FortiGate-1800F	R$ 491.299,57
		FortiGate-1800F Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web Filtering, Antispam Service, and 24x7 Fort	R$ 407.917,86
		Serviço de Instalação	R$ 236.724,64
		Total	**R$ 1.135.942,07**

UNIVERSIDADE FEDERAL DE LAVRAS
REITORIA
SUPERINTENDÊNCIA DE GOVERNANÇA
DIRETORIA DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO
COORDENADORIA DE AQUISIÇÕES DE TECNOLOGIA DA INFORMAÇÃO

3	Razão Social do Fornecedor: APPROACH TECNOLOGIA LTDA CNPJ/CPF: 24.376.542-0001/21 Data: 26/05/2022	NGFW Palo Alto PA-3420	R$ 1.016.257,32
		NGFW Palo Alto PA-3420 - HIGH AVAILABILITY	R$ 1.016.257,32
		Serviço de instalação e configuração do firewall	R$ 37.892,57
		Total	**R$ 2.070.407,21**
Valor Unitário Estimado para o Item 1 (Mediana)		**R$ 1.135.942,07**	

UNIVERSIDADE FEDERAL DE LAVRAS
REITORIA
SUPERINTENDÊNCIA DE GOVERNANÇA
DIRETORIA DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO
COORDENADORIA DE AQUISIÇÕES DE TECNOLOGIA DA INFORMAÇÃO

Tabela de Cálculo do valor estimado para o item 2 da Solução 02

ID	**Pesquisa de Preços -** Licença software de Gerência de Logs e Relatórios Centralizados pelo período de 24 meses.	**DESCRIÇÃO / VALOR**	
1	Razão Social do Fornecedor: NETSOL LTDA CNPJ/CPF: 03.675.909/0001-38 Data: 03/06/2022	02-SSC-9769 SONICWALL ANALYTICS SOFTWARE (SYSLOG) FOR NSA 6700 - 2YR	R$ 11.205,18
2	Razão Social do Fornecedor: IT ONE TECNOLOGIA DA INFORMAÇÃO S.A. CNPJ/CPF: 05.333.907/0001-96 Data: 02/06/2022	FortiAnalyzer-VM Upgrade license for adding 25 GB/Day of Logs and 10 TB storage capacity.	R$ 74.156,46
3	Razão Social do Fornecedor: APPROACH TECNOLOGIA LTDA CNPJ/CPF: 24.376.542-0001/21 Data: 26/05/2022	Software de Gerenciamento e Armazenamento de Logs Centralizado Palo Alto Panorama	R$ 118.519,87
Valor Unitário Estimado para o Item 2 (Mediana)		**R$ 74.156,46**	

UNIVERSIDADE FEDERAL DE LAVRAS
REITORIA
SUPERINTENDÊNCIA DE GOVERNANÇA
DIRETORIA DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO
COORDENADORIA DE AQUISIÇÕES DE TECNOLOGIA DA INFORMAÇÃO

Tabela de Valores Estimados da Pesquisa de Preço para a Solução Viável 03

Item	Descrição	Quant.	Valor Unitário Estimado	Valor Total Estimado
1	Atualização do Firewall Sonicwall Supermassive 9600 para o NSA 5700 e aquisição da licença Essential Protection Service Suite para NSA 5700 em Par de Alta Disponibilidade por 24 meses, com migração do Supermassive 9600 para a nova solução, com serviço mensal de Service Desk prestado pelo fornecedor em regime de 8/5, pelo período de 12 meses.	1	R$ 452.484,47	R$ 452.484,47
2	Aquisição da licença SonicWall Analytics Software pelo período de 24 meses.	1	R$ 9.022,19	R$ 9.022,19
Total Estimado Geral				**R$ 461.506,66**

UNIVERSIDADE FEDERAL DE LAVRAS
REITORIA
SUPERINTENDÊNCIA DE GOVERNANÇA
DIRETORIA DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO
COORDENADORIA DE AQUISIÇÕES DE TECNOLOGIA DA INFORMAÇÃO

Tabela de Cálculo do valor estimado para o item 1 da Solução 03

ID	**Pesquisa de Preços -** Atualização do Firewall SonicWall Supermassive 9600 para o NSA 5700 e aquisição da licença Essential Protection Service Suite para NSA 5700 em Par de Alta Disponibilidade por 24 meses, com migração do Supermassive 9600 para a nova solução, com serviço mensal de Service Desk prestado pelo fornecedor em regime de 8/5, pelo período de 12 meses.	**DESCRIÇÃO / VALOR**	
1	Razão Social do Fornecedor: Netsol LTDA CNPJ/CPF: 03.675.909/0001-38 Data: 03/06/2022	02-SSC-4330 SonicWall NSA 5700 (Secure Upgrade)	R$ 114.106,83
		02-SSC-1715 SonicWall NSA 5700 High Availability (Secure Upgrade)	R$ 110.216,14
		02-SSC-9871 Essential Protection Service Suite for NSA 5700 2yr	R$ 132.879,28
		Serviço mensal de Service Desk prestado pelo fornecedor em regime de 8/5, pelo período de 12 meses.	R$ 43,344,00
		Migração do Supermassive 9600 para o NSA6700.	R$ 8.342,00
		Total	**R$ 408.888,25**
2	Razão Social do Fornecedor: I.M. TECNOLOGIA E SISTEMAS EIRELI CNPJ/CPF: 08.042.908/0001-70 Data: 10/05/2022	02-SSC-4330 SonicWall NSA 5700 (Secure Upgrade)	R$ 130.081,79
		02-SSC-1715 SonicWall NSA 5700 High Availability (Secure Upgrade)	R$ 125.646,40

		02-SSC-9871 Essential Protection Service Suite for NSA 5700 2yr	R$151.482,38
		Serviço mensal de Service Desk prestado pelo fornecedor em regime de 8/5, pelo período de 12 meses.	R$ 57.600,00
		Migração do Supermassive 9600 para o NSA6700.	R$ 13.500,00
		Total	**R$ 478.310,57**
3	Razão Social do Fornecedor: MGSOFT COMÉRCIO E SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO LTDA CNPJ/CPF: 09.493.777.0001-00 Data: 10/05/2022	02-SSC-4330 SonicWall NSA 5700 (Secure Upgrade)	R$ 132.363,92
		02-SSC-1715 SonicWall NSA 5700 High Availability (Secure Upgrade)	R$ 127.850,73
		02-SSC-9871 Essential Protection Service Suite for NSA 5700 2yr	R$ 154.139,96
		Serviço mensal de Service Desk prestado pelo fornecedor em regime de 8/5, pelo período de 12 meses.	R$ 50.400,00
		Migração do Supermassive 9600 para o NSA6700.	R$ 5.500,00
		Total	**R$ 470.254,61**
Valor Unitário Estimado para o Item 1 (Média)		**R$ 452.484,47**	

UNIVERSIDADE FEDERAL DE LAVRAS
REITORIA
SUPERINTENDÊNCIA DE GOVERNANÇA
DIRETORIA DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO
COORDENADORIA DE AQUISIÇÕES DE TECNOLOGIA DA INFORMAÇÃO

Tabela de Cálculo do valor estimado para o item 2 da Solução 03

ID	**Pesquisa de Preços -** Aquisição da licença SonicWall Analytics Software pelo período de 24 meses.	**DESCRIÇÃO / VALOR**	
1	Razão Social do Fornecedor: Netsol LTDA CNPJ/CPF: 03.675.909/0001-38 Data: 03/06/2022	03-SSC-0248 SONICWALL ANALYTICS SOFTWARE (SYSLOG) FOR NSA 5700 - 2YR	R$ 8.201,99
2	Razão Social do Fornecedor: I.M. TECNOLOGIA E SISTEMAS EIRELI CNPJ/CPF: 08.042.908/0001-70 Data: 10/05/2022	3-SSC-0248 SONICWALL ANALYTICS SOFTWARE (SYSLOG) FOR NSA 5700 - 2YR	R$ 9.350,27
3	Razão Social do Fornecedor: MGSOFT COMÉRCIO E SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO LTDA CNPJ/CPF: 09.493.777.0001-00 Data: 10/05/2022	3-SSC-0248 SONICWALL ANALYTICS SOFTWARE (SYSLOG) FOR NSA 5700 - 2YR	R$ 9.514,31
Valor Unitário Estimado para o Item 2 (Média)		**R$ 9.022,19**	

Belo Horizonte, 03 de junho de 2022

Jairo Paviani
Coord. Administração de Redes e Sistemas.
DGTI - Diretoria de Gestão de Tecnologia da Informação.
Universidade Federal de Lavras.

Assunto: **Proposta de Venda e Serviços de Appliances SonicWall**

Objetivo desta Proposta

Esta proposta comercial tem como objetivo especificar as condições oferecidas pela NetSol para a venda, instalação, e manutenção de soluções com equipamento SonicWall.

Valores

Os valores abaixo listados consideram a substituição dos equipamentos ora em uso pela UFLA, Supermassive 9600, em condições promocionais oferecidas pelo Fabricante SonicWall, na opção NSA 6700 com licenças de 2 ou 3 anos.

O terceiro quadro apresenta o valor para a renovação da licença AGSS para Supermassive 9600, atualmente em uso,

NSA 5700 - 2 Anos		
02-SSC-4330	SonicWall NSA 5700 **(Secure Upgrade)**	R$ 114.106,83
02-SSC-1715	SonicWall NSA 5700 High Availability **(Secure Upgrade)**	R$ 110.216,14
02-SSC-9871	Essential Protection Service Suite for NSA 5700 2yr	R$ 132.879,28
03-SSC-0248	SonicWall analytics software (Syslog) for NSA 5700 - 2yr	R$ 8.201,99
		R$ 365.404,24
NSA 5700 - 3 Anos		
02-SSC-4330	SonicWall NSA 5700	R$ 195.027,77
02-SSC-1715	SonicWall NSA 5700 High Availability	R$ 136.490,68
02-SSC-9872	Essential Protection Service Suite for NSA 5700 - 3yr	R$ 188.225,20
03-SSC-0249	SonicWall Analytics Software (Syslog) for NSA 5700 - 3yr	R$ 10.935,99
	Total	**R$ 423.484,16**

Licença Super Massive 9600 - 2 Anos		
01-SSC-1591	Advanced Gateway Security Suite Bundle for Supermassive 9600 2yr	R$ 387.073,83
02-SSC-3965	SonicWall Analytics Software for NSa 9600/NSa 9650 Series 2yr	R$ 17.514,78
	Total	**R$ 404.588,61**

Treinamento, Monitoramento, Relatórios e Service Desk.

Descrição do serviço	Meses	Valor Mensal	Valor Total
Service Desk NetSol (8 x 5) Com plantão até as 24:00 Suporte Ilimitado, Plantão de Emergência, Treinamento Ilimitado, Monitoramento, Backup Diário e Relatórios de Service Desk na nuvem NetSol.	12	R$3.612,00	R$43,344,00
	24	R$3.612,00	R$86.688,00
	36	R$3.612,00	R$130.032,00
Obs.: Este serviço pode ser contratado de forma independente dos demais por 12, 24 ou 36 meses			

Taxa de Instalação e Migração.

Descrição do serviço	Valor Total
Migração do Supermassive 9600 para o NSA6700.	R$8.342,00
OBS.: Este serviço só se aplica no caso da opção por troca do equipamento	

Valores Totais

Resumo Comparativo	Valor Total
Sec. Upgrade NSA 5700 **2 anos** + Hardware, Software, Service Desk NetSol e Migração	R$ 460.434,24
Sec. Upgrade NSA 5700 **3 anos** + Hardware, Software, Service Desk NetSol e Migração	R$ 561.858,16
Renovação Supermassive 9600 **2 anos** + Software e Service Desk NetSol	R$ 491.276,61

Condições Comerciais

Forma de pagamento:	Os valores para a aquisição do(s) equipamento(s) e licenças estão expressos em reais com faturamento direto da NetSol, com vencimento para 28 dias. A cobrança da taxa de Instalação será enviada após a configuração e instalação do(s) equipamento(s).
Contratação dos Serviços	Para a contratação dos serviços basta sua manifestação positiva à NetSol, que providenciará o envio do Acordo de Nível de Serviços a ser assinado entre as partes.
Prazo de Entrega	O prazo de entrega dos equipamentos é de até 40 dias após a solicitação, podendo ocorrer antes caso o distribuidor possua os equipamentos em estoque. Para a entrega das licenças, o prazo é de 10 dias.
Prazo de Instalação	O prazo de instalação dos equipamentos é de até 10 dias úteis a chegada do equipamento sendo acordado entre as partes na assinatura do ANS (acordo de nível de serviço).
Validade da Proposta:	10 dias

Colocamo-nos à disposição para quaisquer esclarecimentos que se fizerem necessários.

Atenciosamente,

Erasmo Borja Sobrinho
Diretor Comercial
erasmo@netsol.com.br
(031) 98835-3505
(031) 3071-8001
NetSol Ltda.
CNPJ: 03.675.909/0001-38

https://www.facebook.com/netsolbrasil - https://linkedin.com/company/475318 - https://twitter.com/netsolbrasil

NetSol
Segurança na Internet

EMPRESA CERTIFICADA
ISO 20000
ISO 27001

Condições Gerais

Ao contratar soluções da SonicWall junto a NetSol, oferecemos profissionais experientes, certificados e em constante atualização que serão usados nas seguintes fases:

Consultoria Especializada e Planejamento

- ✓ Análise do ambiente e dimensionamento dos recursos necessários;
- ✓ Sugestão das melhores práticas de segurança, disponibilidade e conectividade;
- ✓ Definição da solução ideal visando o maior ROI (retorno de investimento);
- ✓ Desenho do novo cenário de rede;
- ✓ Auxílio na busca das melhores condições comerciais para compra de hardware, software e links;
- ✓ Retirada de todas as dúvidas da nova solução junto aos executivos, acionistas, etc;
- ✓ Definição e documentação do escopo de implantação;
- ✓ Treinamento da equipe que for gerenciar a solução;

Implantação/Migração

- ✓ Planejamento da implantação/migração gerando o menor impacto possível;
- ✓ Checklist dos pré-requisitos necessários;
- ✓ Criação do cronograma de atividades;
- ✓ A Instalação é feita de forma remota. Caso o cliente prefira a instalação presencial, é necessária acrescentar as despesas com o deslocamento do técnico ao valor da taxa de instalação.

Suporte

- ✓ SLA (acordo de nível de serviço) de 4 horas;
- ✓ O atendimento é imediato e dirigido diretamente aos analistas responsáveis;
- ✓ A solicitação de suporte ou requisição de serviço pode ser feita pela web ou pelo telefone;
- ✓ No ato da abertura do chamado é solicitado o e-mail do solicitante e o código do atendimento da empresa;
- ✓ No fechamento do chamado, o histórico do mesmo é enviado por e-mail para o responsável que pode avaliar o atendimento recebido;
- ✓ A qualquer momento o cliente pode entrar no Service Desk e consultar todos os chamados que foram abertos, reabrindo um chamado se for desejar;
- ✓ O atendimento é feito para qualquer solicitação durante o horário comercial. A noite e nos finais de semana os clientes podem contar com um telefone de plantão para emergências;
- ✓ Por este atendimento o cliente poderá solicitar ajuda para solucionar os incidentes ocorridos ou efetuar solicitação de serviços, como: criação/alteração no escopo/segmentação de rede, firewall, túneis VPN, balanceamento de links, módulo UTM, sincronização de usuários com o AD, etc;

Manutenção

- ✓ A NetSol irá analisar a necessidade da aplicação de patches de segurança e atualizações de firmware, avisando ao cliente sempre que esta implantação puder gerar alguma instabilidade;
- ✓ Um backup da configuração é feito na NetSol sempre que alguma modificação importante é feita em algum dos equipamentos;
- ✓ O cliente terá também serviços como DNS primário, DNS secundário, DNS reverso, retirada de IP's de blacklists, debug de problemas com links e servidor SMTP de emergência sem nenhum custo adicional;

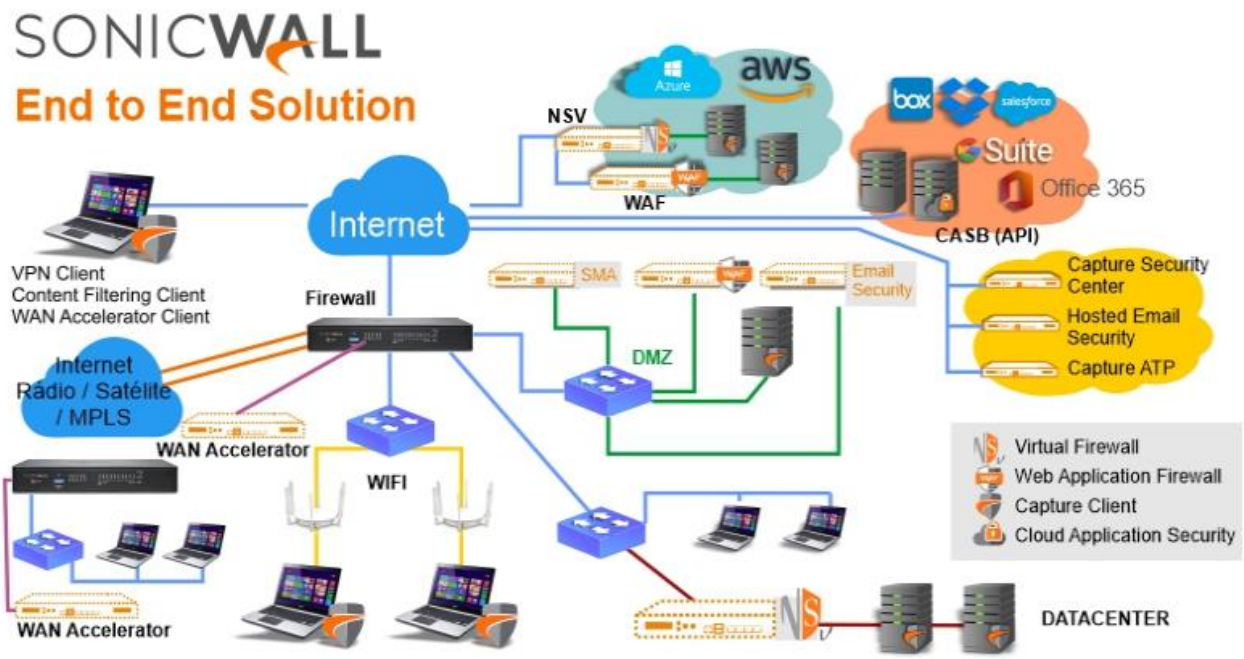
Monitoramento

- ✓ A NetSol monitora todos os equipamentos através de seu Centro de Operações, registrando no Service Desk e informando ao cliente qualquer anormalidade observada;

Treinamento

- ✓ A NetSol irá treinar a equipe de TI do cliente para gerenciar toda a solução sem nenhum custo adicional.
- ✓ Em caso de mudança na equipe de TI, o cliente pode solicitar o agendamento de um novo treinamento;
- ✓ O treinamento pode ser realizado na sede da NetSol em Belo Horizonte ou via join.me.

Sobre a Solução SonicWall Next Generation Firewall



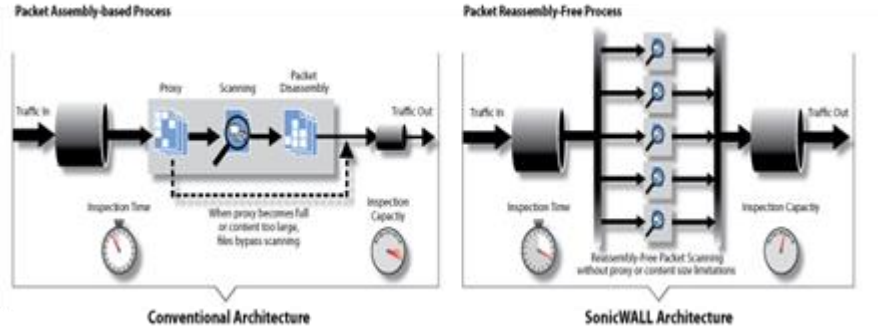
Inteligência de aplicação e controle:

- **Identificação e Controle: Identifica e controla aplicações baseado na tecnologia RFDPI ao invés de depender de portas ou protocolos conhecidos.**
- **Gerenciamento de banda de aplicações:** Aloca banda para aplicações críticas enquanto reduz o consumo de aplicações não-críticas para uso eficiente dos recursos de rede
- **Identificação de Aplicação customizada:** Permite a criação de novas identificações de aplicação, baseado em padrão de tráfego ou parâmetros únicos.
- **Análise de tráfego de aplicações:** Entrega à organização uma visão detalhada do tráfego de rede, consumo de banda e ameaças, além de permitir a identificação de problemas e oferecer ferramentas para análise forense.
- **Base de assinaturas de aplicação:** Uma base que esta continuamente crescendo, com mais de 3.500 aplicações mapeadas, tudo isto para garantir que o administrador será capaz de controlar o uso das mais recentes aplicações, em nível individual ou por categoria.
- **Relatórios IPFIX/Netflow:** Exporte o uso de aplicações através de IPFIX e Netflow para monitoramento através do SonicWall Scrutinizer, ou ferramentas de terceiros. Dados similares podem ser enviados via syslog ao SonicWall GMS e SonicWall Analyzer
- **DPI para SSL:** Tráfego SSL pode ser descriptografado e inspecionado para identificação de *malware* ou intrusos através da tecnologia RFDPI, além disto podem ser aplicadas as políticas de controle de aplicação, URL e conteúdo.
- **Rastreamento de atividade de usuários:** Identificação de usuário é totalmente integrada com *Microsoft Active Directory* e outros sistemas de autenticação, permitindo o rastreamento e relatório de atividades de um usuário específico.

- **Identificação de original de tráfego (GeoIP):** Identifica e controla tráfego de rede com destino ou origem de países específicos.

Proteção de Ameaças no Gateway:

- **Gateway anti-malware:** A tecnologia proprietária RFDPI varre portas e protocolos sem haver limite no tamanho de arquivos. Pesquisadores SonicWall estão constantemente atualizando as proteções contra ataques, provendo respostas rápidas à proteção contra ataques.
- **Reassembly-Free Deep Inspection (RFDPI):** Reassembly-Free Deep Inspection é capaz de detectar Malwares independente da ordem ou tempo em que o pacote chega, permitindo latência extremamente baixa enquanto elimina limitações no tamanho de arquivos, ainda provendo mais desempenho e segurança do que proxys de desenho antigo que remontam conteúdos utilizando conexões amarradas com programas antivírus que causam ineficiência e sobrecarga de memória, resultando em alta latência, baixo desempenho e limitação no tamanho de arquivos que podem ser analisados.



- **Antivírus na nuvem (AV):** Além de utilizar a base de assinaturas carregadas no dispositivo, o RFDPI consulta também a SonicWall Cloud Services para informações adicionais de mais de quatro milhões de assinaturas de *malware*.
- **Inspeção bi-direcional:** RFDPI pode analisar tanto o trafego que entra quanto o que sai, provendo segurança em todas as direções de trafego.
- **Atualizações de assinaturas 24x7:** SonicLabs Research Team cria e atualiza assinaturas de forma constante, estas assinaturas são propagadas para os Firewalls, gerando efeito imediato, sem a necessidade de reinicializações ou interrupção de serviços.

Intrusion Prevention

- **Varredura baseada em assinatura:** O payload dos pacotes é analisado em busca de vulnerabilidades e *exploits* que miram sistemas internos críticos.
- **Atualização automática de assinaturas**: SonicLabs Research Team cria e atualiza assinaturas de forma constante (mais de 5.400 assinaturas, cobrindo 52 categorias de ataque), estas assinaturas são propagadas para os Firewalls, gerando efeito imediato, sem a necessidade de reinicializações ou interrupção de serviços.
- **Prevenção de ameaças na saída:** A habilidade de inspecionar o tráfego de entrada e saída garante que a rede não seja utilizada de forma não intencional para um ataque DDoS e irá prevenir também a comunicação com *Botnets*.
- **Proteção de ataques intra-zone:** A proteção contra ataques pode ser ativada para prevenir ataques internos, originados e destinados à alvos dentro da organização.

VPN

- **IPSec VPN para conexão entre Sites:** Alta performance de VPNs permite que o SuperMassive E10000 seja um concentrador VPN para milhares de conexões com outros grandes sites ou escritórios remotos.
- **SSL VPN ou IPSec cliente:** Utilize *clientless SSL VPN* ou o IPSec Client de fácil gerenciamento para prover acesso à e-mails, arquivos, computadores, sites da intranet e aplicações de diversas plataformas.

- **VPN Gateway redundante:** Quando utilizando mais de uma WAN, uma VPN primária e secundária pode ser configurada para permitir *failover e failback* automático de todas as sessões VPN.
- **Route-based VPN:** A habilidade de realizar roteamento dinâmico sob links VPN garante disponibilidade continua em caso de uma falha temporária de um túnel VPN, re-roteando o tráfego entre *endpoints* através de rotas alternativas.

VOIP

- **Qualidade de Serviço (QoS) avançado:** Garante comunicações críticas com marcação e remarcação 802.1p e DSCP de tráfego VoIP na rede.
- **DPI para tráfego VoIP:** Assinaturas pré-definidas que detectam e bloqueiam ameaças específicas para VoIP.
- **Suporte à H.323 e SIP:** Bloqueia ligações *SPAM* através do bloqueia de ligações que não estejam autorizadas e autenticadas pelo H.323 *gatekeeper* e SIP proxy.

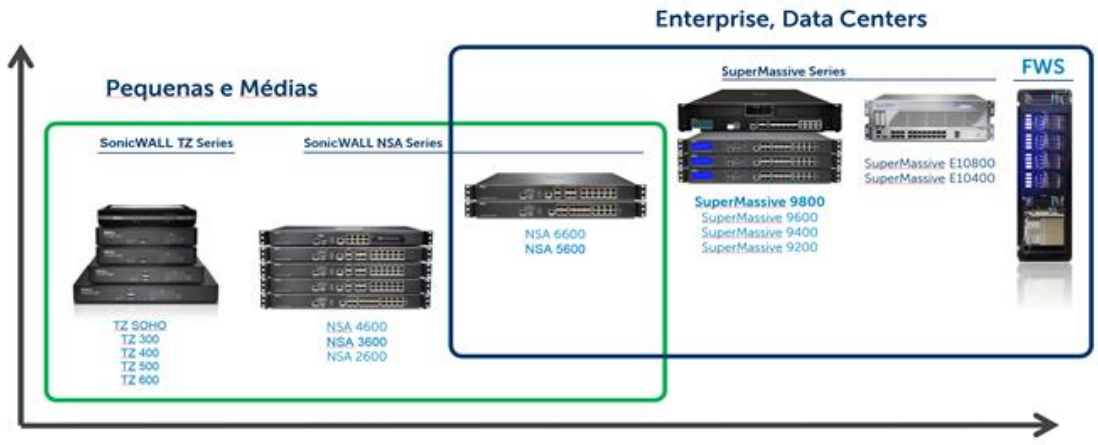
Firewall e Redes

- ***Stateful* Packet Inspection:** Todo tráfego de rede é inspecionado, analizado e colocado em *compliance* com as políticas de firewall.
- **Proteção de ataques distribuídos (DoS):** Proteção de SYN Flood prove defesa contra ataques distribuídos (DoS) usando tanto SYN proxy na camada 3 quando lista negra de SYN na camada 2.
- **Implementação flexível:** Pode ser implementado em NAT tradicional, *Bridge* de camada 2, *Wire Mode*, e *Tap Mode.*
- **Alta disponibilidade (HA):** Suporta stateful Ativo/Passivo, Ativo/Ativo DPI e Ativo/Ativo Clustering Failover para garantir não somente disponibilidade protegendo contra falhas de hardware ou software, mas também aumenta a performance através do compartilhando de carga do RFDPI com as cores disponíveis nas unidades que estiverem em modo de espera (*stand-by).*

Gerenciamento e Monitoramento:

- **WEB GUI:** Interface WEB intuitiva que permite configuração rápida e conveniente, além do gerenciamento através do SonicWall Global Management System (GMS) ou linha de comando.
- **SNMP:** SNMP prove a capacidade de pró-ativamente monitorar e responder à ameaças e alertas.
- **Relatórios IPFIX/Netflow:** Exporte o uso de aplicações através de IPFIX e Netflow para monitoramento através do SonicWall Scrutinizer, ou ferramentas de terceiros. Dados similares podem ser enviados via syslog ao SonicWall GMS e/ou SonicWall Analyzer
- **Gerenciamento centralizado de políticas:** Com o SonicWall GMS, monitore, configure e obtenha relatórios de múltiplos SonicWall appliances a partir de uma única console, de forma intuitiva e customizada.

Portfólio de Equipamentos Security



Sobre a SonicWall

A SonicWall é uma empresa americana com 25 anos de experiência no mercado de segurança e inovação para pequenas e médias redes. Citada pela InfoWorld, PC Magazine, Network World e SC Magazine pela facilidade no uso e alta qualidade e performance de seus appliances. Com mais de 2 milhões de appliances vendidos, é referência no mercado de segurança atestada pelo Gartner, IDC, NSS Labs, ICSA Labs. O appliances SonicWall integram as principais funções de segurança de perímetro incluindo Firewall, VPN IPsec e SSL, IPS, Filtro de Conteúdo Web, Antivírus e Anti-spyware de gateway. Permite integração com o AD e com redes wireless seguras. Também dispõe de recursos para balanceamento e otimização de links..

Referência:

- SonicWall no Site NetSol
- SonicWall Capture Client
- SonicWall Cloud App Security
- SonicWall Secure Mobile Access

Datasheets:

- Datasheet TZ Series
- Datasheet NSa Series
- Datasheet SuperMassive Series
- Datasheet NSv Series

NetSol
Segurança na Internet

EMPRESA CERTIFICADA
ISO 20000
ISO 27001

Sobre a NetSol

A NetSol é uma empresa mineira, fundada no ano 2000, especializada em segurança de redes e internet e tem como missão preservar o ambiente tecnológico de seus clientes.
Para tal, a NetSol presta serviços de alto nível e máxima confiabilidade, com as melhores ferramentas e serviços, mantendo a qualidade personalizada de um atendimento reconhecido pelos clientes por sua excelência.

Nossos Parceiros

A NetSol mantém parceria com diversas empresas afins à atividade de segurança de rede com o objetivo de atender as necessidades de projeto de cada cliente e mantem técnicos treinados a instalar e dar suporte nas soluções:

Acronis, Bitdefender, bitglass, cisco, ESET NOD32, Forcepoint, FORTINET, KASPERSKY lab, Microsoft, MikroTik, RUCKUS, safetica, SOPHOS, SONICWALL, TREND MICRO, ZABBIX, Zimbra Open Source, ubuntu, UniFi, UBIQUITI

Qualidade ISO 20.000-1 e ISO 27.001

A NetSol é das poucas empresas brasileiras certificadas na ISO/IEC 20.000. Esta norma foi editada pela ISO (International Organization for Standardization) especificamente para o correto gerenciamento de serviços de TI. O seu desenvolvimento foi baseado na BS 15000 (British Standard) e tem a intenção de ser inteiramente compatível com o ITIL (Information Technology Infrastructure Library).
Certificada desde 2009, a NetSol vem evoluindo ano a ano na qualidade de sua prestação de serviço e sua excelência é hoje inquestionável, o que e pode ser atestada por seus clientes em constantes pesquisas de satisfação.
Em dezembro de 2021 a NetSol recebeu a certificação da **ISO 27001**, provando que está em conformidade com as normas internacionalmente reconhecidas para **Sistema de Gestão de Segurança da Informação**.

Parceria digital que Transforma.

2021

Ao Cliente

À

A/C: UFLA

Agradecemos a oportunidade e
Apresentamos nossa Proposta Comercial para a Substituição de Produtos SonicWall.

Sobre Nós

Há mais de 20 anos de atuação em **Tecnologia da Informação**, somos **especialistas** em integração. Está em nosso "DNA", ajudar a resolver os desafios de infraestrutura que o seu negócio precisa para **crescer** e sair na frente da concorrência.

Nossa prioridade são nossos clientes. Trabalhamos pela sua satisfação, alinhando **expertise em desenvolvimento** de soluções no mercado corporativo às **melhores práticas**. Ao longo destes anos construímos uma carteira de clientes bem significativa e com muitos casos de sucesso. O próximo pode ser oseu.

Nossa missão como Integrador, é **fornecer soluções para problemas** não usuais e de maior complexidade, relacionados aos **Sistemas de Informação das Organizações**.

1. Objeto

Valores para a troca de equipamentos SonicWall Com as opções para troca do atual NSA 9600 por equipamentos mais atualizados aproveitando a Promoção Secure Upgrade ou a simples renovação de sua licença.

2. Da Proposta de Preços

Nome do proponente, endereço e dados cadastrais:

Rua Rio Grande do Sul, 332, sala 502 - CEP: 41.830-140 - Pituba, Salvador – Bahia

CNPJ -08042908/0001-70

Descrição do serviço: Conforme o item 1 deste documento

Prazo de entrega/execução do serviço: 60 dias

SKU	Descrição	Valor em Real
NSA5700 - 2 Anos		
02-SSC-4330	SonicWall NSA 5700 (Secure Upgrade)	R$130.081,79
02-SSC-1715	SonicWall NSA 5700 High Availability (Secure Upgrade)	R$125.646,40
02-SSC-9871	Essential Protection Service Suite for NSA 5700 2yr	R$151.482,38
03-SSC-0248	SonicWall analytics software (Syslog) for NSA 5700 - 2yr	R$9.350,27
	Total	**R$416.560,84**
NSA5700 - 2 Anos		
02-SSC-4330	SonicWall NSA 5700 (Secure Upgrade)	R$130.081,79
02-SSC-1715	SonicWall NSA 5700 High Availability (Secure Upgrade)	R$125.646,40
02-SSC-9872	Essential Protection Service Suite for NSA 5700 3yr	R$214.576,72
03-SSC-0249	SonicWall Analytics Software (Syslog) for NSA 5700 - 3yr	R$12.467,03
	Total	**R$482.771,94**
NSA6700 - 2 Anos		
02-SSC-4332	SonicWall NSA 6700 (Secure Upgrade)	R$195.384,87
02-SSC-8988	SonicWall NSA 6700 High Availability (Secure Upgrade)	R$185.584,67
02-SSC-9296	Essential Protection Service Suite for NSA 6700 2yr	R$223.802,68
02-SSC-9769	SonicWall Analytics Software (Syslog) for NSA6700 2yr	R$12.773,91
	Total	**R$617.546,13**
NSA6700 - 3 Anos		
02-SSC-4332	SonicWall NSA 6700 (Secure Upgrade)	R$195.384,87
02-SSC-8988	SonicWall NSA 6700 High Availability (Secure Upgrade) (Secure Upgrade)	R$185.584,67
02-SSC-9297	Essential Protection Service Suite for NSA 6700 3yr	R$317.003,48
02-SSC-9770	SonicWall Analytics Software (Syslog) for NSA6700 3yr	R$17.031,88
	Total	**R$ 715.004,90**
Apenas Renovação da Licença NSA9600 - 2 Anos		
01-SSC-1591	Advanced gateway security suite bundle for supermassive 9600 2yr	R$445.919,17
02-SSC-3965	SonicWall analytics software for NSA9600/NSA9650 series 2yr	R$20.177,48
	Total	**R$466.096,65**

Treinamento, Monitoramento, Relatórios e Service Desk.

Descrição	Período	Valor Mensal	Valor Total
Suporte, Plantão de Emergência, Treinamento Ilimitado, Monitoramento, e Relatórios de Service.	24 Meses	R$4.800,00	R$115.200,00

Taxa de Migração.

Serviço	Valor Único
Migração do Supermassive 9600 para o NSA5700 ou NSA6700.	R$13.500,00

Tributos: Incluídos no Valor acima

Condição de pagamento: A vista

Forma de pagamento: Depósito bancário

Validade da Proposta: 30 dias

Salvador, 10 de maio de 2022

_____

Laura Pugliese
Gestão Comercial
I.M. Tecnologia e Sistemas Eireli
CNPJ: 08042908/0001-70

Belo Horizonte, 10 de maio de 2022.

Ao
Sr. Jairo
UFLA
Lavras, MG

PROPOSTA COMERCIAL

Oferecemos soluções completas de firewall, e-mail, datacenter, entre outros serviços, tais como mão de obra qualificada, certificada e treinada pelo fabricante. Atuamos ainda na prestação de serviços de proteção de Redes Corporativas.

Valores

Oferecemos algumas opções para a troca do atual SUPERMASSIVE 9600 ou atualização de licença mantendo o próprio equipamento.

SKU	Descrição	Valor em Real
	NSA 5700 – 2 anos	
02-SSC-4330	SONICWALL NSA 5700	R$ 132.363,92
02-SSC-1715	SONICWALL NSA 5700 HIGH AVAILABILITY	R$ 127.850,73
02-SSC-9871	ESSENTIAL PROTECTION SERVICE SUITE FOR NSA 5700 2YR	R$ 154.139,96
03-SSC-0248	SONICWALL ANALYTICS SOFTWARE (SYSLOG) FOR NSA 5700 - 2YR	R$ 9.514,31
	Total	**R$ 423.868,92**
	NSA 5700 – 3 anos	
02-SSC-4330	SONICWALL NSA 5700	R$ 132.363,92
02-SSC-1715	SONICWALL NSA 5700 HIGH AVAILABILITY	R$ 127.850,73
02-SSC-9872	ESSENTIAL PROTECTION SERVICE SUITE FOR NSA 5700 3YR	R$ 218.341,23
03-SSC-0249	SONICWALL ANALYTICS SOFTWARE (SYSLOG) FOR NSA 5700 - 3YR	R$ 12.685,75
	Total	**R$ 491.241,62**
	NSA 6700 – 2 anos	
02-SSC-4332	SONICWALL NSA 6700	R$ 198.812,68
02-SSC-8988	SONICWALL NSA 6700 HIGH AVAILABILITY	R$ 188.840,54
02-SSC-9296	ESSENTIAL PROTECTION SERVICE SUITE FOR NSA 6700 2YR	R$ 227.729,04
02-SSC-9769	SONICWALL ANALYTICS SOFTWARE (SYSLOG) FOR NSA6700 2YR	R$ 12.998,01
	Total	**R$ 628.380,27**
	NSA 6700 – 3 anos	
02-SSC-4332	SONICWALL NSA 6700	R$ 198.812,68
02-SSC-8988	SONICWALL NSA 6700 HIGH AVAILABILITY	R$ 188.840,54
02-SSC-9297	ESSENTIAL PROTECTION SERVICE SUITE FOR NSA 6700 3YR	R$ 322.564,94

02-SSC-9770	SONICWALL ANALYTICS SOFTWARE (SYSLOG) FOR NSA6700 3YR	R$ 17.330,68
	Total	**R$ 727.548,84**
	Licença para SUPERMASSIVE 9600 – 2 Anos	
01-SSC-1591	ADVANCED GATEWAY SECURITY SUITE BUNDLE FOR SUPERMASSIVE 9600 2YR	R$ 453.742,31
02-SSC-3965	SONICWALL ANALYTICS SOFTWARE FOR NSA9600/NSA9650 SERIES 2YR	R$ 20.531,47
	Total	**R$ 474.273,78**

Taxa de Instalação (Pagamento único)	R$ 5.500,00

Service Desk.

Descrição	Período	Valor Mensal	Valor Total
Serviço de Service Desk - Suporte, Plantão de Emergência, Monitoramento.	24 Meses	R$4.200,00	R$100.800,00

CONDIÇÕES COMERCIAIS

Forma de Pagamento: Boleto bancário

Prazo de Entrega: A entrega ocorrerá em até 30 dias.

Prazo de Instalação: A combinar

Validade da Proposta: Esta proposta tem validade de 15 dias a contar sua data de emissão.

Cordialmente,

Vinícius Leite
Diretor Comercial
MGSOFT COMERCIO E SERV EM TI LTDA
CNPJ 09.493.777.0001-00

Belo Horizonte, 03/06/2022

A/C Jairo Paviani
Universidade Federal de Lavras

Assunto: PROPOSTA 05813 - SONICWALL VENDA + SERVICE DESK

1. OBJETIVO DESTA PROPOSTA

Esta proposta comercial tem por objetivo especificar as condições oferecidas pela NetSol para a venda e suporte de uma solução com de segurança SonicWall.

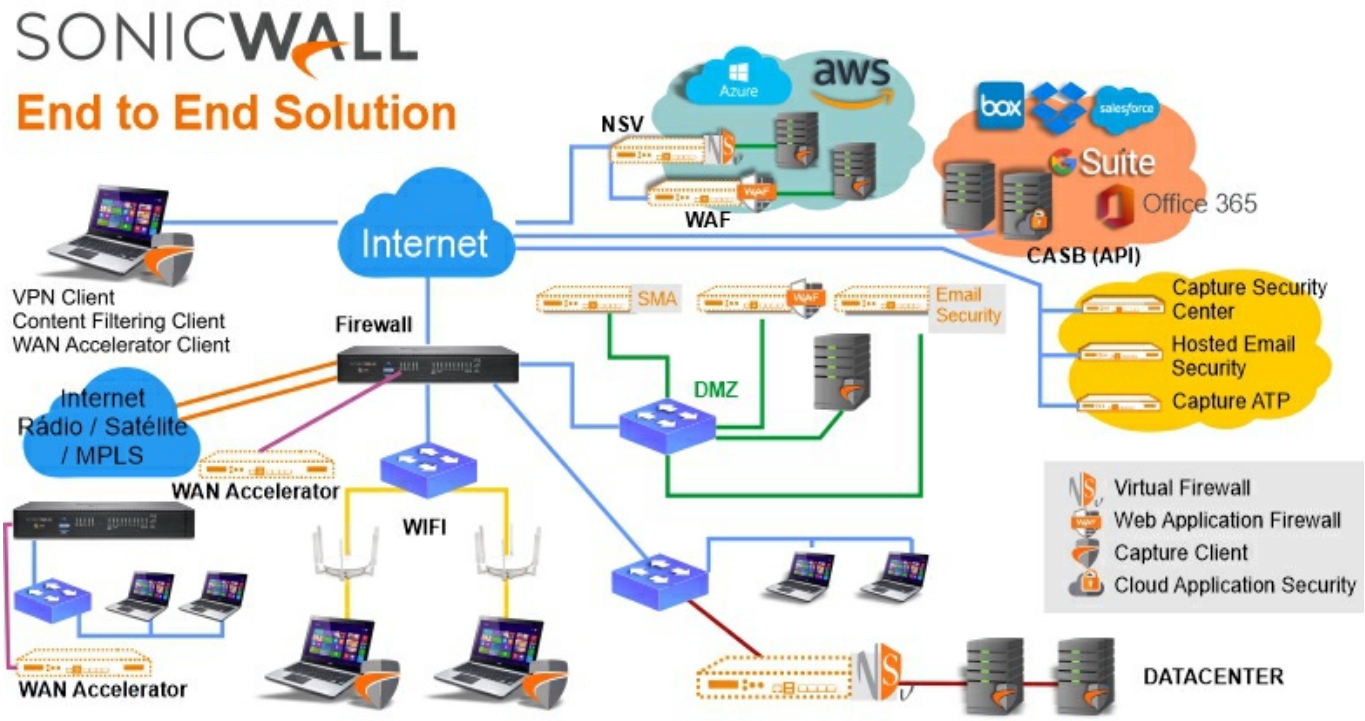


Figura 1 - Soluções SonicWall

2. DADOS DO CLIENTE

Razão Social	Universidade Federal de Lavras
CNPJ	22.078.679/0001-74
Endereço	Câmpus Universitário - Aquenta Sol, Lavras - MG, 37200-900, - - CEP: 37200-900
Cidade / UF	Lavras / Minas Gerais
Representante Legal	Jairo Paviani
Email	jairo.paviani@ufla.br
Telefone	+553538291529

3. VALORES DA VENDA DOS APPLIANCES E LICENÇAS

Item	Quantidade	Unitário	Total
SonicWall - Venda - 02-SSC-4332 SONICWALL NSA 6700 - Sem Sec. Upgrade	1	R$ 294.179,59	R$ 294.179,59
SonicWall - Venda - 02-SSC-8988 SONICWALL NSA 6700 HIGH AVAILABILITY - Sem Sec. Upgrade	1	R$ 205.882,37	R$ 205.882,37
SonicWall - Venda - 02-SSC-9296 Licença ESSENTIAL PROTECTION SERVICE SUITE FOR NSA 6700 2YR	1	R$ 196.318,13	R$ 196.318,13
SonicWall - Venda - 02-SSC-9769 SONICWALL ANALYTICS SOFTWARE (SYSLOG) FOR NSA 6700 - 2YR - Relatórios	1	R$ 11.205,18	R$ 11.205,18
Total	**4**		**R$ 707.585,27**

Itens com faturamento realizado diretamente pela NetSol.

Figura 2 - Linha de Appliances SonicWall

4. VALOR DO SERVIÇO MENSAL

Descrição	Valor Mensal
Serviço mensal de service desk (treinamento/suporte/monitoramento/administração) sem limite de horas. Item opcional.	R$ 3.612,00

5. VALOR DA TAXA DE INSTALAÇÃO

Descrição	Valor Único
Migração do Supermassive 9600 para o NSa 5700. Item opcional.	R$ 8342,00

6. CONDIÇÕES GERAIS

Ao contratar soluções da SonicWall junto a NetSol, oferecemos profissionais experientes, certificados e em constante atualização que serão usados nas seguintes fases:

Consultoria Especializada e Planejamento

- Análise do ambiente e dimensionamento dos recursos necessários;
- Sugestão das melhores práticas de segurança, disponibilidade e conectividade;
- Definição da solução ideal visando o maior ROI (retorno de investimento);
- Desenho do novo cenário de rede;
- Auxílio na busca das melhores condições comerciais para compra de hardware, software e links;
- Retirada de todas as dúvidas da nova solução junto aos executivos, acionistas, etc;
- Definição e documentação do escopo de implantação;
- Treinamento da equipe que for gerenciar a solução;

Implantação/Migração

- Planejamento da implantação/migração gerando o menor impacto possível;
- Checklist dos pré-requisitos necessários;
- Criação do cronograma de atividades;
- A Instalação é feita de forma remota. Caso o cliente prefira a instalação presencial, é necessária acrescentar as despesas com o deslocamento do técnico ao valor da taxa de instalação.

Suporte

- SLA (acordo de nível de serviço) de 4 horas;
- O atendimento é imediato e dirigido diretamente aos analistas responsáveis;
- A solicitação de suporte ou requisição de serviço pode ser feita pela web ou pelo telefone;
- No ato da abertura do chamado é solicitado o e-mail do solicitante e o código do atendimento da empresa;
- No fechamento do chamado, o histórico do mesmo é enviado por e-mail para o responsável que pode avaliar o atendimento recebido;
- A qualquer momento o cliente pode entrar no Service Desk e consultar todos os chamados que foram abertos, reabrindo um chamado se for desejar;
- O atendimento é feito para qualquer solicitação durante o horário comercial.
- Na parte da noite e nos finais de semana os clientes podem contar com um telefone de plantão para emergências;
- Por este atendimento o cliente poderá solicitar ajuda para solucionar os incidentes ocorridos ou efetuar solicitação de serviços, como: criação/alteração no escopo/segmentação de rede, firewall, túneis VPN, balanceamento de links, módulo UTM, sincronização de usuários com o AD, etc;

Manutenção

- A NetSol irá analisar a necessidade da aplicação de patches de segurança e atualizações de firmware, avisando ao cliente sempre que esta implantação puder gerar alguma instabilidade;
- Um backup da configuração é feito na NetSol sempre que alguma modificação importante é feita em algum dos equipamentos;
- O cliente terá também serviços como DNS primário, DNS secundário, DNS reverso, retirada de IP’s de blacklists, debug de problemas com links e servidor SMTP de emergência sem nenhum custo adcional;

Monitoramento

- A NetSol monitora todos os equipamentos através de seu Centro de Operações, registrando no Service Desk e informando ao cliente qualquer anormalidade observada;

7. CONDIÇÕES COMERCIAIS

Razão Social: NetSol LTDA	**CNPJ: 03.675.909/0001-38**
Forma de pagamento	
Contratação dos serviços	Para a contratação dos serviços basta sua manifestação positiva à NetSol, que providenciará o envio do Acordo de Nível de Serviços a ser assinado entre as partes.
Prazo de entrega	O prazo de entrega dos equipamentos é de até 60 dias após a solicitação, podendo ocorrer antes caso o distribuidor possua os equipamentos em estoque. Para a entrega das licenças, o prazo é de 10 dias.
Prazo de instalação	O prazo de instalação dos equipamentos é de até 10 dias úteis a chegada do equipamento sendo acordado entre as partes
Validade da proposta	10 dias - válida até 13/06/2022.
Termo de Confidencialidade	Este documento, assim como seu conteúdo, deve ser tratado como propriedade confidencial, não podendo ser divulgado a terceiros ou reproduzido de forma parcial ou integral sem prévia autorização e aprovação da NetSol. Informações técnicas e comerciais eventualmente obtidas durantes a realização das atividades envolvidas nesta proposta comercial, como especificação, funcionamento ou planos de ação a serem executados são igualmente confidências e sigilosas.

8. SOBRE A SONICWALL

A SonicWall é uma empresa americana com 25 anos de experiência no mercado de segurança e inovação para pequenas e médias redes. Citada pela InfoWorld, PC Magazine, Network World e SC Magazine pela facilidade no uso e alta qualidade e performance de seus appliances. Com mais de 2 milhões de appliances vendidos, é referência no mercado de segurança atestada pelo Gartner, IDC, NSS Labs, ICSA Labs. O appliances SonicWall integram as principais funções de segurança de perímetro incluindo Firewall, VPN IPsec e SSL, IPS, Filtro de Conteúdo Web, Antivírus e Anti-spyware de gateway. Permite integração com o AD e com redes wireless seguras. Também dispõe de recursos para balanceamento e otimização de links.

Referência:

- SonicWall no Site NetSol
- SonicWall Capture Client
- SonicWall Cloud App Security
- SonicWall Secure Mobile Access

Datasheets:

- Datasheet TZ Series
- Datasheet NSa Series
- Datasheet SuperMassive Series
- Datasheet NSv Series

9. SOBRE A NETSOL

A NetSol é uma empresa mineira, sediada em Belo Horizonte, fundada no ano 2000, especializada em segurança de redes e internet e tem como missão preservar o ambiente tecnológico de seus clientes.

Para tal, a NetSol presta serviços de alto nível e máxima confiabilidade, com as melhores ferramentas e serviços, mantendo a qualidade personalizada de um atendimento reconhecido pelos clientes por sua excelência.

A NetSol é das poucas empresas brasileiras certificadas na ISO/IEC 20.000. Esta norma foi editada pela ISO (International Organization for Standardization) especificamente para o correto gerenciamento de serviços de TI. O seu desenvolvimento foi baseado na BS 15000 (British Standard) e tem a intenção de ser inteiramente compatível com o ITIL (Information Technology Infrastructure Library).

Certificada desde 2009, a NetSol vem evoluindo ano a ano na qualidade de sua prestação de serviço e sua excelência é hoje inquestionável, o que e pode ser atestada por seus clientes em constantes pesquisas de satisfação.

Em dezembro de 2021 a NetSol recebeu a certificação da **ISO 27001**, provando que está em conformidade com as normas internacionalmente reconhecidas para **Sistema de Gestão de Segurança da Informação**.

10. NOSSOS PARCEIROS

A NetSol mantém parceria com diversas empresas afins à atividade de segurança de rede com o objetivo de atender as necessidades de projeto de cada cliente e mantem técnicos treinados a instalar e dar suporte nas soluções.

11. SIGA-NOS NAS REDES SOCIAIS

Estas são as nossas principais redes sociais:

https://www.facebook.com/netsolbrasil https://linkedin.com/company/475318 https://twitter.com/netsolbrasil

Colocamo-nos à disposição para quaisquer esclarecimentos que se fizerem necessários.

Atenciosamente,

Diretoria
NetSol Ltda
Site: https://www.netsol.com.br
Email: contato@netsol.com.br
Telefone: +55-31-3071-8001

IT ONE
YOUR DIGITAL FUTURE TODAY

Proposta Técnica Comercial_

UFLA

PROJETO FIREWALL

Belo Horizonte, 02/06/2022 I Proposta: PR-14082 I Versão 03

Índice

4003-3716
www.itone.com.br
contato@itone.com.br

Rua Alberto Cintra, 161
6º Andar I União - Belo Horizonte
MG I 31160-370

1. Propriedade

Restrições de Uso e Divulgação da Proposta

As informações contidas em todas as folhas desta proposta são confidenciais, sejam elas técnicas, financeiras ou comerciais. As informações fornecidas à UFLA não podem ser usadas ou divulgadas sem prévia autorização da IT-One para propósitos que não sejam os de avaliação da proposta.

Da mesma forma, a IT-One compromete-se a não divulgar ou fornecer dados e informações referentes aos fornecimentos realizados, a menos que expressamente autorizado pela UFLA, mantendo absoluta confidencialidade em relação às atividades desenvolvidas.

As propostas da IT-One poderão ser submetidas via e-mail e mídia eletrônica para sua conveniência. Se o conteúdo diferenciar entre as cópias impressa e o formato eletrônico, o conteúdo da impressa será garantido pela IT-One.

2. Institucional

Quem é a IT-One e como podemos ajudar sua empresa

Fundada em 2002 na cidade de Belo Horizonte e contando com mais de 150 colaboradores, a IT-One é uma empresa com foco em soluções inovadoras e de alto valor agregado para Infraestrutura de Tecnologia da Informação que oferece ao mercado os melhores produtos, serviços gerenciados, soluções em nuvem (privada, pública ou híbrida) e consultoria.

Atuando em praticamente todo o território nacional, a IT-One é reconhecida pela experiência em projetos de TI, pelo time de profissionais certificados e por uma oferta completa de hardware, software e serviços que atendem às principais necessidades de tecnologia em seus clientes de todos os portes e segmentos, contribuindo decisivamente para o aumento da eficiência operacional e para a redução de custos e de riscos através de soluções inteligentes e customizadas.

A IT-One, um dos maiores integradores de soluções em TI do Brasil, está pronta para ajudar a sua empresa a enfrentar seus desafios de negócios e os impactos gerados pela "TRANSFORMAÇÃO DIGITAL".

Onde estamos localizados

Possuímos presença local nas cidades de Belo Horizonte, Brasília, Goiânia, Indaiatuba, Recife, Rio de Janeiro, São Paulo e Uberlândia, oferecendo aos nossos clientes um atendimento personalizado e com agilidade.

4003-3716
www.itone.com.br
contato@itone.com.br

Rua Alberto Cintra, 161
6º Andar I União - Belo Horizonte
MG I 31160-370

3. Solução Proposta

3.1. Escopo solicitado

Projeto Network Firewall.

Item 01 – Firewall de Nova Geração

- Fortigate 1800F – Appliance Físico
- FortiGate-1800F Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web Filtering, Antispam Service)
- Interfaces
    - 2 x GE RJ45 MGMT Ports
    - 2 x 10 GE SFP+ / GE SFP HA Slots
    - 16 x GE RJ45 Ports
    - 8 x GE SFP Slots
    - 12 x 25 SFP28 / 10 GE SFP+ / GE SFP Slots
    - 4 x 40 GE QSFP+ Slots
- Desempenho do Sistema — Combinação de Tráfego Corporativo
    - IPS Throughpu – 17 Gbps
    - NGFW Throughput – 11 Gbps
    - Threat Protection Throughput – 9.1 Gbps
- Desempenho e capacidade do sistema
    - IPv4 Firewall Throughput – 140 Gbps
    - IPv6 Firewall Throughput – 140 Gbps
    - Concurrent Sessions (TCP) – 12 Milhões
    - New Sessions/Second (TCP) – 750.000
    - Firewall Policies – 100.000
    - IPsec VPN Throughput – 55 Gbps
    - Concurrent SSL-VPN Users – 10.000
    - SSL Inspection Throughput – 12 Gbps
    - SSL Inspection Concurrent Session – 1.3 Milhões
    - Application Control Throughput – 34 Gbps
    - CAPWAP Throughput – 26.5 Gbps
    - Maximum Number of FortiAPs – 4.096
    - Maximum Number of FortiTokens – 20.000
    - Fonte Redundante

- Transceivers
    - 1 Gbps – 4 Unidades (SKU-FN-TRAN-LX)
    - 10 Gbps – 2 Unidades (SKU-FN-TRAN-SFP+LR)

Subitem 1.1 GARANTIA E SUPORTE FABRICANTE

- A solução está sendo fornecida com o software e com a licença irrestrita, em sua versão mais atual e completa.
- O fabricante está sendo condicionado com suporte 24x7, fornecendo abertura de chamados no portal online e telefone 0800 em casos de emergência.
- O fabricante disponibiliza documentos nos quais ajuda com documentações e bases de conhecimentos para que a solução sempre tenha os recursos necessários em sua funcionalidade.
- É disponibilizado pelo fabricante de forma pública, acessos aos guias de ajudas e documentos online que podem ser utilizados pelo time da UFLA-MG.
- A solução ofertada, Firewall Fortigate possui garantia de 24 (vinte e quatro) meses com um período de disponibilidade para chamada de manutenção de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.
- A UFLA-MG poderá abrir chamados de manutenção diretamente no fabricante, sem a necessidade de prévia consulta e/ou qualquer liberação por parte da ITONE. Não havendo limite para aberturas de chamados, sejam de esclarecimentos de dúvidas sobre a configuração e a utilização da solução ofertada.
- A abertura de chamados poder ser realizada através de telefone 0800 do fabricante ou pela ITONE, ou através da página da WEB do fabricante e endereço de e-mail do fabricante.
- Documentação digital, publicada pelo fabricante da solução ofertada.

Item 3 – Serviço de Implementação da Solução

Serviço de instalação e configuração, Gerenciamento de projetos.

- A IT-One irá disponibilizar 1 (um) gerente de projeto responsável por acompanhar a instalação e configuração dos equipamentos. Seguem as responsabilidades deste profissional:
  - Fazer uma reunião de alinhamento e overview do escopo do projeto, gerenciamento de expectativas, planos de comunicação e requisitos necessários para implementação;
  - Realizar a coleta de todas as informações necessárias para elaboração da arquitetura de implementação;
  - Verificar se o ambiente atende todos os requisitos de hardware e software;

- Fazer a análise e definição da Arquitetura de Implementação, baseada nas melhores práticas de mercado em conjunto com a equipe da UFLA-MG;
- Análise e mitigação de riscos ao negócio;
- Estimativa de impacto e janelas de indisponibilidade;
- Validação da instalação e configuração dos equipamentos, no local, em ondas definidas em acordo com a UFLA-MG;
- Entrega da Arquitetura de Implementação para validação técnica do UFLA-MG;
- Após a validação técnica da Arquitetura de Implementação, deverá ser enviado o cronograma do projeto;

- **Escopo de execução:**
  - Cadastro do e-mail institucional no Portal Fortinet / Aplicação da Licença nos equipamentos
  - Atualização de Firmware Fortigate 1800F
  - Configurações Integração com Active Directory / Configuração das Portas Custom para Gestão do Firewall (HTTP/HTTPS/SSH)
  - Configuração de até 300 (trezentas) políticas de verificação e correção de postura;
  - Configuração de até 300 (trezentas) políticas de segmentação de rede;
  - Criação de até 5 (cinco) Network Devices Profiles;
  - Configuração do SDWAN / Configura de 30 Profiles - DNS Filter/IPS/SSL Inspection/ Application Control
  - Criação e Configuração de 60 Vlans
  - Criação e Configuração de 60 rotas estáticas
  - Configuração de 3 Políticas - Dos Policy IPV4 / Configuração VPN / 3 Profile SSL - VPN
  - Configuração de 5 túneis VPN - Site to Site
  - Configuração de VPN Client to Site
  - Configuração do envio de logs para o FortiCloud
  - Repasse de Conhecimento
  - Operação Assistida durante 05 dias úteis.
  - Documentação do Projeto
  - Entrega do Termo Aceite Final

Subitem 3.1 - Central de registros e chamados ITONE

- Atendimento chamados via 0800 e canais disponibilizados para o contrato;
- Registro de chamados em sistema interno, para clientes em contrato;
- Registro de chamado em fabricante, caso o contrato do cliente necessite/permita;
- Acompanhamento do SLA do atendimento do time IT-ONE ou do time do parceiro;
- Histórico de chamados registrados para o contrato. Diagnósticos, avaliações e resolução de problemas;
- Escalonamentos de chamados no portal do fabricante

Opcionais:

1) FortiAnalyzer-VM Upgrade license for adding 25 GB/Day of Logs and 10 TB storage capacity.

O FortiAnalyzer é um poderoso gerenciador de logs, análise e plataforma de relatórios, fornecendo às organizações um painel único orquestração, automação e resposta para segurança simplificada operações, identificação proativa e remediação de riscos, e visibilidade completa de toda a superfície de ataque.

- Subscription license 24 meses for 25 GB/Day
- Storage capacity Central Logging & Analytics
- Include 24x7 FortiCare Support

2) Suporte Técnico complementar ao do fabricante – 500 horas (banco de horas)

- Dúvidas em configurações realizadas
- Análise de Logs
- Atualização de Firmware
- Abertura de chamados no fabricante
- Serviço sob demanda.

4. Termos e Condições Comerciais

4.1.Preços

Condições comerciais para HW, SW e Serviços ofertados:

Hardware, Software e Serviços:

ITEM	DESCRIÇÃO	TIPO FATURAMENTO	QTDE	VALOR UNITÁRIO	VALOR TOTAL
1	FortiGate-1800F	HW	1	491.299,57	R$ 491.299,57
2	FortiGate-1800F Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web Filtering, Antispam Service, and 24x7 Fort	SV	1	407.917,86	R$ 407.917,86
3	Serviços Instalação	SV	1	236.724,64	R$ 236.724,64
TOTAL					**R$ 1.135.942,07**

OPCIONAIS:

ITEM	DESCRIÇÃO	TIPO FATURAMENTO	QTDE	VALOR UNITÁRIO	VALOR TOTAL
1	FortiAnalyzer-VM Upgrade license for adding 25 GB/Day of Logs and 10 TB storage capacity.	SV	1	74.156,46	R$ 74.156,46
2	Suporte complementar fabricante - 500 hs	SV	1	225.000,00	R$ 225.000,00
TOTAL					**R$ 299.156,46**

Dólar utilizado como referência = 5,20

Marcos de Faturamento de Serviços:

Fase/Etapa	Descrição	%
Aceite da Proposta	Comercial	20%
Transição / Execução	Plano de Arquitetura e Cronograma do Projeto	20%
	Entrega ambiente de Desenvolvimento / Homologação com termo de aceite parcial	20%
	Entrega ambiente de Produção com termo de aceite parcial	20%
Ongoing	Aceite Final do Projeto	20%

* Os marcos de faturamento serão acordados e confirmados entre o gerente de projeto da IT-One com os responsáveis do cliente.

Cliente é contribuinte ICMS? ( ) Sim (X) Não

*Os preços dos produtos apresentados estão expressos em reais. ou

4.2. Validade

Esta proposta é válida por 30 (trinta) dias.

Os preços dos itens ofertados estão expressos em reais e a IT-One poderá rever a validade desta Proposta sempre que ocorrer um fato ou ato superveniente que resulte na imposição de um ônus excessivo refletido nos valores e preços mencionados. Nesse caso, esta Proposta perderá sua validade, ficando facultado à IT-One emitir nova proposta ou revalidar os termos desta Proposta, o que será feito formalmente. Nesse caso, esta Proposta perderá sua validade, ficando facultado à IT-One emitir nova Proposta ou revalidar os termos desta Proposta, o que será feito formalmente.

Essa proposta comercial não poderá, em hipótese alguma, ser considerada como estimativa para processo licitatório caso a validade esteja expirada e/ou a cotação do Dólar (BACEN – PTAX) tenha variação de 2 pontos percentuais no período compreendido entre o dia da emissão desta Proposta e o dia final de validade da mesma.

Caso a referida proposta seja considerada para estimativa de processo licitatório, mesmo se enquadrando nos casos acima descritos, ocorrendo diferença entre o preço nela contido e o ofertado no processo, prevalecerá o último (preço ofertado no processo licitatório). Não podendo, em hipótese alguma, o Pregoeiro(a) condicionar a nossa classificação ou desclassificação no processo a manutenção dos preços aqui expressos.

4.3. Termos e Condições contratuais

Aos produtos e serviços aqui ofertados aplicam-se os "Termos e Condições Contratuais – IT-One", registrado no 2º Ofício de Registro de Títulos e Documentos da Comarca de Belo Horizonte, protocolado sob o nº 1188070 em 06 de outubro de 2015.

4.4. Prazo de entrega

90 (noventa) dias após o recebimento formal do pedido de compras (Contrato e/ou Empenho e/ou AF e/ou Pedido formal).

4.5. Pagamento

Em até 30 dias após a entrega dos equipamentos ou serviços/emissão da NF.

Projeto de Segurança da Informação

Cliente: UFLA

26 de maio de 2022

Eduardo Mazzochi
Executivo de contas
mazzochi@approachtec.com.br | 48 99621-7551

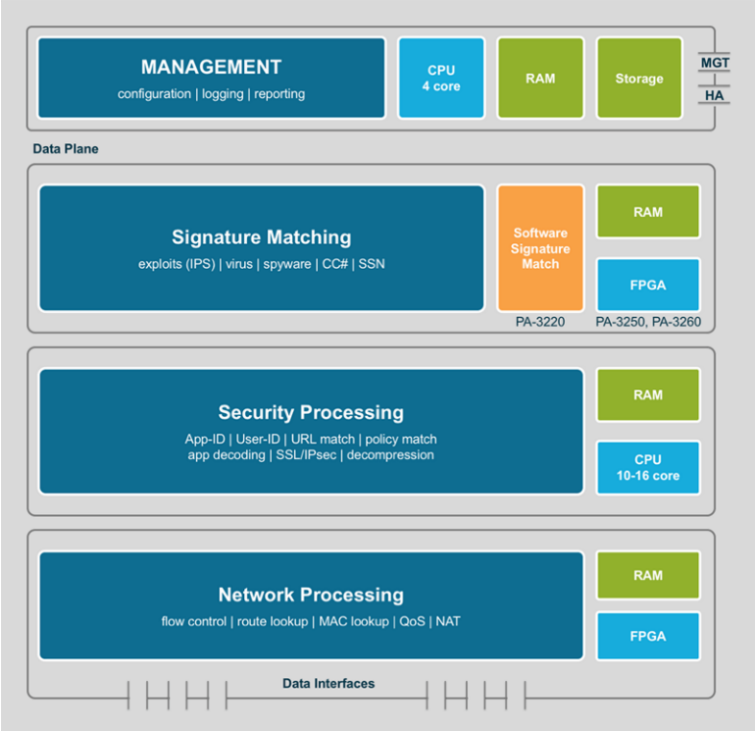
1. Descrição do projeto

O projeto proposto compreende o fornecimento de solução de segurança da informação com appliances de firewall de próxima geração (NGFW), software de gerenciamento e armazenamento de logs Panorama, serviço de instalação e configuração e treinamento para atender as demandas da UFMG

Solução Firewall de Próxima Geração

A solução de Firewall de Próxima Geração da Palo Alto fornece recursos de hardware dedicados e programáveis para funções de rede, segurança, correspondência de assinaturas e gerenciamento, garantindo excelente e inigualável desempenho. Os equipamentos Palo Alto oferecem alta taxa de decodificação e capacidade de sessão SSL para que você possa proteger o tráfego criptografado sem diminuir a velocidade dos negócios, simplificar suas implantações, descobrir e interromper ameaças ocultas sem comprometer a privacidade.

A arquitetura de hardware da solução é robusta e permite alto desempenho em tempo real, pois possui processadores dedicados para cada função, executando todas funções de rede e proteção em um único appliance.



Principais recursos de segurança de um Firewall de Próxima Geração

- Classifica todos os aplicativos, em todas as portas, o tempo todo.
- Identifica o aplicativo, independentemente da porta, da criptografia (SSL ou SSH) ou das técnicas evasivas utilizadas.
- Usa o aplicativo, não a porta, como base para todas as suas decisões sobre a política de ativação segura: permitir, negar, agendar, inspecionar e aplicar a formatação do tráfego.

- Categoriza aplicativos não identificados para controle da política, estudo forense de ameaças ou desenvolvimento de tecnologia do App-ID™.
- Aplica as políticas de segurança para qualquer usuário, em qualquer local.
- Implanta políticas consistentes para os usuários locais e remotos que usam as plataformas Windows®, Mac® OS X®, Linux®, Android® ou Apple® iOS.
- Permite a integração sem agente com o Microsoft® Active Directory® e serviços de terminal, LDAP, Novell® eDirectory™ e Citrix®.
- Integra facilmente as suas políticas de firewall ao 802.1X sem fio, proxies, soluções NAC e qualquer outra fonte de informações sobre a identidade do usuário.
- Bloqueia ameaças conhecidas e desconhecidas.
- Bloqueia uma série de ameaças conhecidas, incluindo explorações, malware e spyware, em todas as portas, independentemente das táticas de evasão de ameaças comuns empregadas.
- Limita a transferência não autorizada de arquivos e dados confidenciais e habilita de forma segura a navegação na Web não relacionada ao trabalho.
- Identifica malware desconhecido, analisa-o com base em centenas de comportamentos maliciosos e, em seguida, cria e entrega a proteção automaticamente.

Reconhecimento Palo Alto

A Palo Alto é reconhecida 8 vezes consecutivas como Líder no Mercado de NGFW (Next Generation Firewall) de acordo com o **Gartner**.

1.1. Escopo técnico

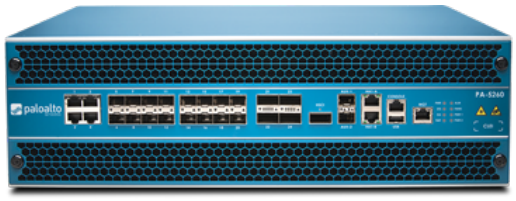
O estudo foi realizado com base nos dados levantados em reuniões e apresentações com o cliente, com objetivo de desenvolver um projeto robusto, escalável e seguro. A partir dessas informações os equipamentos adequados às necessidades da UFMG foram sugeridos conforme segue nesta proposta.

1.1.1. Cenário Proposto

- Dois Firewalls de Próxima Geração Palo Alto PA-3420, com fonte de alimentação redundante, para operação em um cluster de alta disponibilidade, com suporte e garantia pelo período de 03 (três) anos, incluindo atualização do sistema operacional, correção de bugs, e troca do equipamento ou peças em caso de problema;
- Licença de Threat Prevention para firewall Palo Alto PA-3420, com subscrição de 3 (três) anos, para proteção contra Ameaças Conhecidas utilizando recursos como Antivírus, IPS e Anti-Spyware;
- Licença de URL Filtering para firewall Palo Alto PA-3420, com subscrição de 3 (três) anos, para filtro de conteúdo baseado em categorias de sites e URLs e proteção contra acesso a sites maliciosos e sites tipo phishing;
- Licença de WildFire para firewall Palo Alto PA-3420, com subscrição de 3 (três) anos, para proteção contra Ameaças Avançadas (Zero Day) através do uso de machine learning para análise dinâmica no próprio firewall e análise em sandbox na nuvem;
- Licença de GlobalProtect para firewall Palo Alto PA-3420, com subscrição de 3 (três) anos, habilitando recursos avançados de VPN e disponibilizando o acesso ao software cliente de VPN desenvolvido pela Palo Alto Networks para computadores com sistemas operacionais MS Windows, MacOS e Linux e dispositivos móveis iOS e Android;
- Software Palo Alto Panorama para gerenciamento centralizado e armazenamento de logs de forma ilimitada, sem limite de tempo ou espaço utilizado, para gerenciar até 25 dispositivos, com 03 (três) anos de suporte e atualizações;
- Serviço de Instalação e Configuração de todos os componentes da solução;
- Treinamento presencial de 40 horas, realizado nas dependências da UFMG, ministrado por técnico certificado nas soluções Palo Alto sobre administração e utilização da solução;

1.1.2. Equipamentos propostos

1.1.2.1. Firewall modelo PA-3420 para o Site Principal



PA-3420

1. Firewall throughput measured with App-ID and logging enabled utilizing 64KB HTTP/appmix transactions
2. Threat Prevention throughput measured with App-ID, IPS, antivirus, anti-spyware, WildFire and logging enabled utilizing 64KB HTTP/appmix transactions.
3. IPsec VPN throughput measured with 64KB HTTP transactions.
4. New sessions per second measured with application-override utilizing 1-byte HTTP transactions and logging enabled.

Ref: https://www.paloaltonetworks.com/products/product-comparison?chosen=pa-3420

2. Itens e valores

Item	Fabricante	Modelo	Descrição	Qtd	Valor Unit.	Valor Total
1	PALO ALTO	PA-3420	NGFW Palo Alto PA-3420 com 36 meses de garantia Premium do fabricante	2	R$ 1.016.257,32	R$ 2.032.514,63
2	PALO ALTO	PANORAMA	Software de Gerenciamento e Armazenamento de Logs Centralizado Palo Alto Panorama com 36 meses de garantia Premium do fabricante	1	R$ 118.519,87	R$ 118.519,87
3	APPROACH	INSTALAÇÃO	Serviço de Instalação e Configuração de Firewall	1	R$ 37.892,57	R$ 37.892,57
4	PALO ALTO	EDU-210	Voucher Individual para Participação no Treinamento Oficial de Firewall Palo Alto	4	R$ 15.460,17	R$ 61.840,67
					Subtotal	R$ 2.250.767,74

3. Condições comerciais

- **Prazo de entrega:** Em até 90 (noventa) dias após a confirmação do pedido.
- **Validade da proposta:** 30 (trinta) dias**.**

4. Confidencialidade

As informações contidas nesta proposta são confidenciais e fornecidas para a finalidade exclusiva de apresentação técnica e comercial da Approach Tecnologia a pedido do cliente, e não deve, de forma alguma, ser utilizada para qualquer outra finalidade.

Atenciosamente,

Eduardo Mazzochi
Executivo de contas
mazzochi@approachtec.com.br | 48 99621-7551