Processo/Ano **Histórico do Processo**

240/ 2018 LICENÇAS DE USO E SUPORTE TÉCNICO ESPECIALIZADO PARA AS FERRAMENTAS DE FIREWALL E PROXY DE BORDA. CONSIDERANDO AS CRESCENTES AÇÕES DE ATAQUES VIRTUAIS IMPETRADAS POR CRACKERS E O EFETIVO FUNCIONAMENTO DA SOLUÇÃO ORA CONTRATADA, SOMADOS À QUALIDADE DO SUPORTE TÉCNICO PRESTADO, TAL OBJETO TORNOU-SE IMPRESCINDÍVEL NA ESTRUTURA DESTA INSTITUIÇÃO. **CONTRAÇÃO ANUAL - PERIODO 9 MESES EM 2018 E 3 MESES PARA 2019**

Data Solicitação/Empenho

20//03/2018

Fornecedor

103207 – NETDEEP TECNOLOGIA LTDA - ME

Unidade Solicitante

ACESSORIA DE INFORMÁTICA

PREFEITURA DA ESTÂNCIA TURÍSTICA DE SÃO ROQUE

Rua São Paulo, 966 - Bairro Taboão - CEP.: 18.135-125 - São Roque/SP

Fone: (11) 4784-8530 / 4784-8532 - Fax: (11) 4712-024 - CNPJ: 70.946.009/0001-75

EMISSÃO DE SOLICITAÇÃO

SOLICITAÇÃO Nº. 1306 **DATA:** 15/03/2018

SOLICITANTE: 011939 - MAXWEL DA SILVA LIMA
CARGO: AUXILIAR ADMINISTRATIVO
FUNÇÃO: CHEFE DE DIVISAO
CONTRATO: 0/-1 **ATA:**

DESTINO: LICENÇAS DE USO E SUPORTE TÉCNICO ESPECIALIZADO PARA AS FERRAMENTAS DE FIREWALL E PROXY DE BORDA. CONSIDERANDO AS CRESCENTES AÇÕES DE ATAQUES VIRTUAIS IMPETRADAS POR CRACKERS E O EFETIVO FUNCIONAMENTO DA SOLUÇÃO ORA CONTRATADA, SOMADOS À QUALIDADE DO SUPORTE TÉCNICO PRESTADO, TAL OBJETO TORNOU-SE IMPRESCINDÍVEL NA ESTRUTURA DESTA INSTITUIÇÃO.

RECURSO ORÇAMENTÁRIO

FICHA: 39 **DOTAÇÃO:** 01.01.05.04.122.0008.2008.3.3.90.39.00
Fonte Recurso: 001 - Tesouro
Cód Aplicação: 110.0000 - GERAL

ORÇADO	SUPLEMENTADO	RESERVADO	EMPENHADO	LIQUIDADO	PAGO	SALDO
1.400.000,00	236.800,00	6.335,46	1.559.077,73	267.043,80	9.543,80	71.386,81

SERVICOS

Item	Descrição	Fmt	U.E.	QtdeEmb	Qtde	Vlr.Unit.	Total
1	006.001.0263 - CONTRATAÇÃO DE SOLUÇÃO DE FIREWWALL E PROXY COMPLETA COM IMPLANTAÇÃO, TREINAMENTO, SUPORTE, MANUTENÇÃO E CONSULTORIA EM SEGURANÇA DE REDES		SE	0	9	508,33	4.574,97

Total Solicitação **4.574,97**

011939 - MAXWEL DA SILVA LIMA
Departamento de Informática
SOLICITANTE

013646 - ISAIAS GOMES DOS SANTOS
DIRETOR DE DEPARTAMENTO
TECNICO DE INFORMATICA

Memorando 186/2017

Para: Serviço de Compras - Sr. David Silveira

Assunto: Manifestação sobre possível renovação do objeto que trata o Processo 520/2017

Referente ao objeto que trata o **Processo 520/2017**, informo que trata-se de serviços ligados à segurança da informação (digital).

Tais recursos compreendem a disponibilização de licenças de uso e suporte técnico especializado para as ferramentas de *firewall* e *proxy* de borda em uso por esta Prefeitura. Considerando as crescentes ações de ataques virtuais impetradas por *crackers* e o efetivo funcionamento da solução ora contratada, somados à qualidade do suporte técnico prestado, tal objeto tornou-se imprescindível na estrutura desta instituição. Através destas ferramentas, é possível manter o ambiente de redes da Prefeitura mais seguro e estável, além de gerir os usuários e seus respectivos acessos à Internet e promover auditoria no uso de tal recurso em alinhamento com a Lei Federal 12.965/14 ("Marco Civil da Internet") e o Decreto Municipal 7283/2011.

Isto posto, informamos a necessidade de continuidade na contratação do objeto em questão também para o ano de 2018.

São Roque, 01 de dezembro de 2017.

SOLUÇÃO DE FIREWALL E PROXY

Sumário

Isaías Gomes dos Santos
Diretor de Informática
RG: 45.127.633-4

Isaías Gomes dos Santos
Diretor de Informática
RG: 45.127.633-4

Isaías Gomes dos Santos
Diretor de Informática
RG: 45.127.633-4

Isaías Gomes dos Santos
Diretor de Informática
RG: 45.127.633-4

ESPECIFICAÇÃO TÉCNICA

1. Objeto

Contratação de **Solução de Firewall/Proxy (SFP)** com *interface* de gerenciamento WEB e suporte a até 600 (seiscentas) contas de usuários "logados" simultaneamente; devendo ser fornecido com consultoria em segurança de redes, licenciamento e atualização da solução, treinamento de utilização, garantia, suporte técnico e manutenção pelo período mínimo de 01 (um) ano.

2. Características Gerais da Solução

2.1. Sistema Operacional

2.1.1. Introdução às Necessidades do Sistema Operacional

A **Solução de Firewall/Proxy (SFP)** a ser adquirida pela Prefeitura da Estância Turística de São Roque deverá possuir rotinas completas de sistema operacional, podendo este ser de terceiros ou proprietário, dando a possibilidade mínima de administrar e gerenciar os recursos relacionados abaixo.

2.1.2. *Boot* do Sistema

a. Para as rotinas de inicialização ou desligamento do sistema em caso de alguma necessidade de manutenção em específico, deverá ser também disponibilizada opção via ambiente gráfico para ação de reinicialização e desligamento do sistema.

2.1.3. *Interface* de Gerenciamento

a. Todo o acesso à **SFP** deverá ser realizado via *interface* WEB (HTTP/HTTPS) gráfica. Isto inclui sua manutenção, elaboração e manutenção de regras, emissão de relatórios, configurações, rotinas de backup, gerência de serviços, entre outros;
b. Para acesso aos níveis de funcionalidade **SFP**, deverá ser permitida a elaboração de usuários com níveis hierárquicos, onde os mesmos poderão ou não ter permissões de acesso aos módulos da solução conforme definições realizadas pelo(s) usuário(s) administrador(es).

2.1.4. Relógio do Sistema

a. Visando manter a exatidão nas rotinas e a precisão na documentação com relação ao LOG de eventos e outras intervenções, o relógio do sistema deverá permitir ser configurado de forma manual ou automática, por intermédio de sincronismo com servidores NTPs na WEB ou em rede local;
b. Deverá permitir que o sincronismo seja agendado ou não pelo administrador.

2.1.5. Gerenciamento de Serviços

a. Para melhor gerenciamento do servidor e sua rotina de trabalho, a **SFP** deverá possuir *interface* gráfica WEB para interação com os serviços, sendo possível visualizar *status* do serviço (ativo ou parado);
b. Deverá permitir administrar completamente os serviços inerentes à ela;

Isaías Gomes dos Santos
Diretor de Informática
RG: 45.127.633-4

c. Deverá permitir a suspensão e/ou reativação do serviço pelo administrador do sistema sempre que necessário.

2.1.6. *Interfaces* de Rede

a. Nas *interfaces* de redes existentes no sistema da **SFP**, deverá ser possível a alteração manual dos endereços IP, visando a customização da solução conforme necessidade do administrador;
b. Deverá ser possível a elaboração de novas *interfaces* virtuais para as possíveis demandas que o servidor venha a ser exposto, sendo que estas poderão ser removidas a qualquer momento;
c. Também deverá ser permitida a configuração das *interfaces* para os serviços específicos de uma solução *firewall/proxy* completa, tais como: *interface* para LAN, para WAN (Internet) e DMZ.

2.1.7. Placas de Rede

a. O sistema operacional da **SFP** deverá armazenar e informar o fabricante, o modelo, o *MAC address* e a capacidade máxima de tráfego de dados das placas de rede conectadas ao *hardware* no qual será instalada;
b. Deverá dar suporte à interação de configuração, seja de forma automática manual, com os tipos de comunicação das *interfaces* de rede do *hardware* (se *half duplex* ou *full duplex*);
c. Deverá exibir o *status* da conectividade de placas de rede, informando se há ou não cabo à elas conectados;
d. Permitir, apenas de forma manual, a troca das *interfaces* de rede conforme necessidades da Prefeitura da Estância Turística de São Roque.

2.1.8. *Backup* e Restauração

a. Visando a segurança e continuidade nos serviços da **SFP**, a mesma deverá ter inerente à sua estrutura uma ferramenta de *backup* e restauração de suas configurações;
b. A ferramenta de *backup* deverá realizar cópias de segurança das configurações *default* de toda a estrutura do servidor;
c. Deverá realizar cópia de segurança dos arquivos de auditoria dos pacotes que por ela passarem;
d. Os *backups* deverão poder ser realizados via FTP, pasta de rede compartilhada, localmente no próprio servidor/*hardware* ou por meio de sincronismo dinâmico com local remoto;
e. Deverá ser possível agendar as rotinas de *backups* de forma que os mesmos possam ocorrer diariamente, semanalmente ou mensalmente;
f. Deverá ser possível configurar qual dia da semana e horário a rotina/tarefa de *backup* será executada;
g. Para todas as rotinas de *backup* realizadas, deverá também ser permitida a execução da restauração dos arquivos *"backupeados"*, tais como: restauração do LOG de auditoria e das configurações implementadas.

2.1.9. Failover e Clusterização

a. Visando a alta disponibilidade da **SFP**, seu sistema deve ser compatível com técnica de *failover*, permitindo a realização "clusterização" com outro *hardware* que utilize a mesma solução. Isto, caso a Prefeitura da Estância Turística de São Roque opte pela aquisição de outra licença.

Isaías Gomes dos Santos
Diretor de Informática
RG: 45.127.633-4

2.1.10. Saúde do Sistema Operacional

a. Visando uma maior monitoria de todo o servidor, o **SFP** deverá emitir relatórios em tempo real do *status* de *hardware* e seus serviços, sendo possível o acompanhamento e verificação em modo gráfico de informações de configurações, tais como: sistema operacional, memória RAM, processador e memória SWAP (se houver);
b. Deverá ser emitido gráficos sobre o estado de uso do(s) HD(s) do *hardware*;
c. Verificação das bases de todos os serviços implementados que armazenem dados;
d. Deverá ser permitido, via ambiente gráfico, realizar correção das tabelas de base de dados que, eventualmente, possam vir a corromper-se;
e. Dever ser permitida, seja de forma manual ou automática/agendada, a limpeza dos LOGs de auditoria gerados pelo sistema.

2.1.11. Compatibilidade com *Hardware* de Instalação

a. O sistema operacional da **SFP** deverá ser compatível com os *hardwares* comuns de mercado que utilizem plataforma i386, não havendo a necessidade de nenhum *appliance* especial para o correto funcionamento de suas funcionalidades.

2.2. Alta Disponibilidade e Balanceamento de *Links*

2.2.1. Introdução Sobre o Serviço de Balanceamento de *Links*

Visando melhor utilização, interoperabilidade e continuidade quanto aos recursos de acesso à Internet, a **Solução de Firewall/Proxy (SFP)** deve permitir que mais de um *link* de dados seja vinculado à ela e que o balanceamento de carga entre estes *links* seja implementado conforme necessidade da Prefeitura da Estância Turística de São Roque. Para isto, os parâmetros abaixo devem ser suportados.

2.2.2. Monitoramento

a. Uma vez implementado, todos os *links* vinculados ao servidor da **SFP** devem ser monitorados por ele;
b. Deve possibilitar testes de endereço IP, sendo que este poderá ser inserido/vinculado manualmente;
c. Deve permitir testes de *link* de Internet, visando saber se o mesmo está ativo ou não, permitindo, inclusive, a programação prévia da ação de testes sobre o *link*, conforme necessidade da Prefeitura da Estância Turística de São Roque;
d. Todo o monitoramento de *link* deve ser realizado em tempo real;
e. Deve emitir alerta automático em caso de queda repentina do(s) *link(s)* de Internet vinculado(s) à solução.

2.2.3. Tabela de *links*

a. A infraestrutura da **SFP** deve permitir a redundância dos *links* de dados a ela vinculados;
b. Também deverá permitir o balanceamento de carga entre os *links* de dados vinculados.

2.2.4. Redundância

a. Deve permitir que regras de redundância sejam elaboradas e inseridas manualmente na **SFP**, conforme a necessidade da Prefeitura da Estância Turística de São Roque;

Isaías Gomes dos Santos
Diretor de Informática
RG: 45.127.633-4

b. Deve permitir a configuração de ordem dos *links* vinculados ao servidor.

2.2.5. Balanceamento

a. A **SFP** deve permitir a elaboração de regras de balanceamento de carga de dados manualmente, conforme necessidades da Prefeitura da Estância Turística de São Roque.

2.3. *Firewall*

2.3.1. Introdução ao *Firewall* de Borda

A **Solução de Firewall/Proxy (SFP)** deverá contar com um serviço de *firewall* completo e flexível, e possuir tecnologias e recursos mais comumente utilizados atualmente no mercado, de forma que permita a elaboração de regras, controles de rede e de portas, implementação de IDS/IPS, entre outros, conforme descrito nesta especificação.

2.3.2. Regras de *Firewall*

a. Para as regras a serem elaboradas na **SFP**, deverá ser permitida a liberação de entradas e saídas individuais para cada uma;
b. Deve ser permitido aplicar nomenclaturas individuais às regras elaboradas;
c. Deve ser permitida a alteração de forma individual das *interfaces* às quais as regras se aplicam;
d. Permitir a liberação de regras com opções de protocolos individualmente separados;
e. Permitir a elaboração de regras por grupos ou redes de endereços IP;
f. Permitir elaborar opções para as regras de forma que as mesmas sejam efetivas, ou agendadas, ou temporárias, ou regras fixas;
g. Permitir saber o *status* de cada uma das regras em uso ou não;
h. Possibilitar realizar ações sobre as regras já existentes ou em elaboração, de forma que seja possível parar, reativar, remover ou atualizá-las;
i. Realizar a impressão de relatórios das regras já elaboradas e/ou em uso no momento.

2.3.3. Controle de Redes

a. A **SFP** deverá permitir a liberação ou bloqueio de endereços IP e/ou portas entre as redes (LAN, WAN, DMZ) e *subnets* da Prefeitura da Estância Turística de São Roque;
b. Permitir a liberação ou bloqueio de portas específicas para endereços IP de conexões via VPN realizadas ao servidor ou que passem por ele com destino a outro equipamento;
c. Permitir que liberações ou bloqueios sejam feitos por *range* de endereços IP;
d. Permitir que nomes sejam atrelados individualmente a cada uma das regras de controle de redes das previamente elaboradas, facilitando a manutenção e interação com as mesmas.

2.3.4. Agendamento

a. Visando otimizar as rotinas e aplicações do serviço de *firewall* da **SFP**, o sistema deverá permitir o agendamento de configurações manuais de ajustes ou alterações de regras;
b. Devem poder ser feitos de modo diário, semanal e mensal;
c. Devem permitir que sejam indicados os horários iniciais e finais para ações a serem efetuadas sobre as regras.

Isaías Gomes dos Santos
Diretor de Informática
RG: 45.177.633-4

2.3.5. Cadastro de Portas

a. Visando facilitar a manutenção para os cadastros das portas ou serviços à elas relacionados, o administrador poderá nomear as regras implementadas ao invés de apenas o número das portas. Assim, o administrador poderá basear-se em nomes e não em números, o que facilita a ação e a diminuição do tempo de resolução de incidentes.

2.4. IDS e IPS

2.4.1. Introdução aos Serviços de IDS e IPS

Visando a segurança em todo o parque da Prefeitura da Estância Turística de São Roque, a **Solução de Firewall/Proxy (SFP)** deverá possuir tecnologia e inteligência de detecção e prevenção de ataques embarcados em sua estrutura – serviços estes comumente classificados como IDS e IPS –, sendo que tais recursos deverão atender às seguintes ações e demandas de funcionamento conforme relação abaixo.

2.4.2. Ferramenta

a. Deve fazer análise por assinatura dos pacotes que passarem por ele;
b. Realizar o filtro em *layer* 7, bloqueando pacotes que usem portas aleatórios ou diferente da porta padrão de determinado protocolo;
c. Deve fazer análise por eventos ocorridos no tráfego de dados e pacotes que passarem pela **SFP**;
d. Permitir que as tecnologias de IDS e IPS sejam implementadas por *interfaces* de rede do sistema/*hardware* de forma individual;
e. Permitir a edição de categorias e suas respectivas assinaturas;
f. Permitir a ativação ou desativação do serviço conforme necessidades do administrador;
g. Realizar o monitoramento de detecção e prevenção em *full time* e em *background*;
h. Deverá ter em sua estrutura o serviço de NIDS para detecção de intrusão na rede, sendo que este deverá fazer uso de ferramentas e rotinas com algoritmos de inspeção baseados em regras pré-definidas, sem falso-positivo e com controle total do refinamento das regras;
i. Deverá possuir metodologia de detecção multidimensional que verifique as assinaturas (impressões digitais) de possíveis ataques, anomalias de protocolos em tráfego e anomalias comportamentais dos pacotes e cargas de protocolo;
j. A função de NIDS poderá ser habilitada ou desabilitada para inicialização junto com o sistema, bem como poderá ser ativada ou desativada pelo administrador e deverá possuir indicação de *status* onde, através deste, será possível verificar se o serviço está ou não ativo.

2.5. Regras de QoS

2.5.1. Introdução ao Serviço de QoS

Considerando as necessidades da Prefeitura da Estância Turística de São Roque, a **Solução de Firewall/Proxy (SFP)** deverá permitir a implementação do serviço de QoS. Para isto, os parâmetros e itens de configuração relacionados abaixo deverão ser suportados.

Isaías Gomes dos Santos
Diretor de Informática
RG: 45.127.633-4

2.5.2. Configuração de Parâmetros de *Link*

a. Visando melhor utilização dos *links*, deverá ser permitida a configuração de velocidade real dos *links* de Internet para cada *link* utilizado, conforme necessidade da Prefeitura da Estância Turística de São Roque;
b. Deve permitir também a configuração de QoS – *Traffic Shaping*, visando diminuir a perda de pacotes e de uso de banda.

2.5.3. Divisão do *Link*

a. O sistema da **SFP** deverá prover a possibilidade de adicionar regras de QoS manualmente;
b. Permitir implementar índice de prioridades para as regras mais importantes;
c. Permitir configurar regras independentes para *download* e *upload*;
d. Permitir, de forma gráfica, a divisão de banda de cada *link*;
e. Deve permitir a personalização de *rate* mínimo e *rate* máximo para cada regra elaborada;
f. Uma vez que uma regra já tenha sido elaborada, a aplicação deve permitir modificações de valores na composição da mesma.

2.5.4. Parâmetros para Configuração de Regras

a. As regras elaboradas dentro da **SFP** devem permitir o uso de portas de saída e/ou portas de entrada em sua composição;
b. Deve permitir elaboração de regras utilizando endereços IP internos específicos;
c. Deve haver a disponibilidade para adicionar diversas portas em uma única regra.

2.6. VPN

2.6.1. Introdução à Conexão VPN

A **Solução de Firewall/Proxy (SFP)** a ser contratada pela Prefeitura da Estância Turística de São Roque deve possuir suporte à redes VPN seguras, sendo aceito acessos via Intranet, Extranet e Conexão Remota, e deverá dar suporte aos itens abaixo relacionados.

2.6.2. VPN

a. Deverá utilizar a estrutura de VPN, sendo que a autenticação da conexão ponto-a-ponto a ser estabelecida deverá utilizar chaves secretas compartilhadas, certificados digitais e autenticação com usuário e senha;
b. O serviço de VPN deverá possibilitar a utilização no modo *multiclient-server* de forma que o cliente conectado utilize a autenticação pública com certificados digitais, sendo que isto deve ser provido através de assinaturas digitais e certificados de autoridade;
c. Deverá ter suporte de forma extensiva à criptografia aberta *OpenSSL* e utilizar também os protocolos SSLv3/TLSv1 no estabelecimento e permanência de comunicação.

2.6.3. Parâmetros de Configurações da VPN

a. Deve permitir acesso ao usuário de VPN individual;
b. Deve permitir que o endereço IP da VPN seja fixado;
c. Permitir conexão entre servidores de forma automática, desde que previamente implementado pelo administrador do sistema;

Isaías Gomes dos Santos
Diretor de Informática
RG: 45.127.633-4

d. Possuir mecanismo que envie, via e-mail, o certificado e manual de instalação da VPN a quem estará do outro lado ponta da conexão, de forma que o mesmo possa proceder com instalação dos requisitos de acesso seguro;
e. Permitir que o usuário "logado" na VPN seja desabilitado pelo administrador do sistema se necessário;
f. Possibilitar que a *range* de endereços IP inseridos na VPN seja alterada conforme a necessidade do administrador do sistema;
g. Imprimir relatórios com as contas vinculadas e/ou inseridas na VPN;
h. Ser compatível e permitir criptografia através dos protocolos 3DES (168 bits) e AED (256 bits), suportando também o protocolo *diffie-hellman* com performance mínima de 1.0 Gbps para ambos os protocolos, além dos protocolos SSLv3/TLSv1;
i. Ter compatibilidade com os sistemas operacionais: *Microsoft Windows* 10, *Windows* 7 (x86/x64), *Windows Vista* (x86/x64) *Windows* 8/8.1 (x86/x64) e Linux (nas diversas distribuições existentes no mercado).

2.6.4. Compatibilidade

a. **SSL** – Compatível com sistemas operacionais *Microsoft Windows* 7, *Vista*, 8, 8.1 (x86/x64) e Linux em suas diversas distribuições, permitindo ser configurado por usuário individual, por endereço IP automático ou manual, com possibilidade de fixar e alterar *range* de endereços IPs da VPN;
b. **IPSEC** – Permitindo ser acessado por usuário individual e com criptografia com segredo compartilhado ou chave RSA.

2.6.5. Monitoramento

a. O serviço de VPN da **SFP** deve possuir monitoramento em tempo real de conexões em atividade;
b. Deve possibilitar a identificação do endereço IP externo da rede que se conectou a ela;
c. Informar o horário em que a conexão ocorreu e sua durabilidade.

2.6.6. Segurança

a. A VPN da **SFP** deve permitir a elaboração de políticas de acesso e controle individuais ou por grupo de dispositivos;
b. Permitir elaboração de políticas de controle entre as redes de VPN e LAN;
c. Emitir relatórios de históricos de conexões à VPN realizados por cada usuário.

2.7. *Proxy* de Navegação

2.7.1. Introdução ao Servidor *Proxy*

Visando segurança, melhor uso de banda e menor impacto possível à infraestrutura de rede da Prefeitura da Estância Turística de São Roque, a **Solução de Firewall/Proxy (SFP)** deverá dar suporte à implementação do serviço de *Proxy* para navegação dos usuários, conforme os itens descritos abaixo.

Isaías Gomes dos Santos
Diretor de Informática
RG: 45.127.633-4

2.7.2. Modo de Operação de Usuários no *Proxy*

a. A **SFP** deverá permitir implementar '*Proxy* transparente' e '*Proxy* autenticado' para validação de acesso à Internet dos usuários da Prefeitura da Estância Turística de São Roque. Sendo que para o:

2.7.2.1. *Proxy* Transparente

a. Os usuários devem ser validados com referências individuais;
b. Deverá permitir implementar grupos e diretivas de navegação por endereçamento IP ou *MAC address* das estações de trabalho;
c. Deve permitir a impressão de relatórios de listas de usuários e grupos de navegação;
d. Para o *Proxy* transparente, deverá ser possível aplicar os métodos de autenticação de usuário dos tipos: Base local, AD/OpenLDAP (NTLM ou LDAP) Smbauth, PAM, MSNAUTH.

2.7.2.2. Proxy Autenticado

a. Os usuários devem ser validados com credenciais individuais;
b. Deve permitir implementar grupos e diretivas de navegação por credenciais (*logins*) de acesso à Internet;
c. Deve permitir a impressão de relatórios de listas dos usuários e grupos de navegação;
d. Deve ser possível colocar campo de observação individual para cada credencial de usuário, visando favorecer a documentação sobre eventuais ações tomadas sobre as mesmas;
e. Permitir a liberação ou bloqueio com possibilidade de mais de uma *range* de endereçamento IP simultaneamente.

2.7.3. Grupo de Navegação

a. Deve permitir a implementação de diversos grupos de navegação, onde regras isoladas para cada um deles poderão ser aplicadas;
b. Deve possibilitar a configuração de horários para ativação das regras sobre os grupos de navegação;
c. Deve permitir a elaboração de múltiplas regras no mesmo grupo de navegação;
d. Deve possibilitar a visualização das regras de navegação elaboradas em ambiente gráfico.

2.7.4. Regras de Navegação

a. A **SFP** deverá dar suporte a elaboração de regras de navegação de forma ilimitada e conforme as necessidades da Prefeitura da Estância Turística de São Roque;
b. Deve possibilitar a elaboração de regras por categorias de acesso. Para estas, deve ser permitido o bloqueio, a liberação e a exceção das categorias elaboradas;
c. Deve permitir a elaboração de regras sobre domínios. Para estas, deve ser permitido o bloqueio, a liberação e exceção de domínios vinculados;
d. Possibilitar a elaboração de regras por "palavras". Para estas, deve ser permitido o bloqueio e a exceção das "palavras" utilizadas;
e. Possibilitar a elaboração de regras por extensão de arquivos. Para estas, deve ser permitido o bloqueio e a exceção das extensões aplicadas.

Isaías Gomes dos Santos
Diretor de Informática
RG: 45.327.633-4

2.7.5. Listas

a. A **SFP** deverá dar suporte à elaboração de listas vinculadas às regras de navegação, conforme as necessidades da Prefeitura da Estância Turística de São Roque;
b. Deve permitir que estas listas sejam por domínio, por palavras e por extensões. Todas devem ser personalizáveis pelo administrador do sistema, conforme necessidade da Prefeitura da Estância Turística de São Roque.

2.7.6. Controle de Navegação

a. Visando o melhor uso do(s) *link*(s) de Internet da Prefeitura da Estância Turística de São Roque, a **SFP** deverá permitir a implementação de controle do tempo de navegação realizada pelos usuários à ela vinculados;
b. Realizar o filtro, classificação e controle em *layer* 7, de forma as aplicações que estejam trabalhando com portas aleatórios ou diferente da porta padrão de determinado protocolo trazendo potenciais riscos à infraestrutura da Prefeitura da Estância Turística de São Roque, sejam bloqueados;
   Deverá realizar controle de tempo de utilização do acesso à Internet, onde será possível criar políticas de horários e tempo de acesso;
c. Permitir a elaboração de controle de utilização de banda de navegação por grupo de usuário;
d. Permitir elaboração de política para bloqueio ou não de *downloads* de arquivos considerando seus respectivos tipos (executáveis, imagens, filmes, músicas, entre outros);
e. Permitir o filtro de cabeçalhos MIME das páginas acessadas, visando a restrição de conteúdo impróprio.

2.7.7. Antivírus

a. A **SFP** deverá possuir inerente à sua estrutura uma solução antivírus que consiga detectar e bloquear códigos maliciosos na navegação realizada pelos usuários;
b. Visando não haver restrições que gerem impactos negativos, deverá ser possível a implementação de regras de forma também que URLs de *sites* da Internet nelas inseridas não passem pela rotina de análise do antivírus do servidor.

2.7.8. Liberação por Endereço IP

a. Deve possibilitar a implementação de configuração por unidade ou por grupo de forma que determinadas URLs de *sites* da Internet não necessitem de autenticação no *Proxy*;
b. Deve permitir também a impressão de relatórios das listas de URLs de *sites* da Internet alocados a cada regra elaborada de liberação por endereço IP.

2.7.9. CACHE

a. O serviço de *Proxy* da **SFP** deverá permitir implementar o CACHE de *sites* da Internet que foram utilizados em navegações de usuários, visando velocidade e economia de banda;
b. Também deve permitir a configuração de URLs de *sites* da Internet de forma que estes não armazenem CACHE no servidor;
c. Deve permitir que seja realizada a limpeza manual do CACHE de *sites* da Internet armazenados;
d. Deve ser possível personalizar manualmente o tamanho máximo do armazenamento em CACHE;
e. Deve permitir personalizar o tamanho máximo do CACHE de memória;

Isaías Gomes dos Santos
Diretor de Informática
RG: 45.127.633-4

f. Deve permitir personalizar o tamanho máximo do arquivo que será armazenado em CACHE.

2.7.10. Mensagens aos Usuários

a. A **SFP** deve permitir implementar rotinas de mensagem automática ao usuário no caso da URL do *site* da Internet em que ele está tentando acessar esteja bloqueada pelo serviço de *Proxy* da solução;
b. Deve permitir implementar rotinas de mensagens de alertas de monitoramento personalizadas destinadas ao administrador do sistema ou usuários previamente cadastrados para recebe-las.

2.8. Demais Serviços/Servidores de Rede da Solução

2.8.1. Introdução aos Demais Serviços/Servidores de Rede da Solução

Caso haja necessidade, a **Solução de Firewall/Proxy (SFP)** deve permitir que outros serviços/servidores de rede possam ser implementados em sua infraestrutura, conforme necessidade da Prefeitura da Estância Turística de São Roque. Sendo estes serviços/servidores relacionados abaixo.

2.8.2. Servidor DHCP

a. A **SFP** deve possibilitar a implementação de um servidor DHCP para que endereçamentos IP sejam distribuídos aos *hosts* do parque;
b. Deverá permitir a configuração manual do serviço de DHCP;
c. Permitir a fixação de *ranges* inicial e final em uma faixa de endereçamento preestabelecida;
d. Deve possibilitar a interação com um domínio já existente, sendo possível relação de DNS primário e DNS secundário, *getway*, fixação de endereçamento de *broadcast*, interação e implementação de servidor *Wins*, configuração de tempo padrão e limite para disponibilização de um único endereço IP aos *hosts* do parque;
e. Deve ser permitida a configuração de reservas de endereços IP para *hosts* em específico, sendo que estas devem ser efetuadas através do *MAC address* do *host* a que se destine.

2.8.3. Servidor DNS

a. A **SFP** deve possibilitar a implementação de servidor DNS, onde neste poderão ser elaborados mais de um domínio para interação;
b. Deve ser possível fazer apontamentos de *hosts* e de outros domínios;
c. Permitir a implementação de DNS inverso;
d. Permitir a limpeza de *cache* dos domínios DNS nele implementados;
e. Realizar a impressão de relatórios dos apontamentos de DNS e os endereços IP a ele devidamente vinculados.

2.8.4. Rotas de Rede

a. Considerando a função de *getway* e *firewall* que a **SFP** possuirá, a mesma deverá permitir a implementação de rotas de redes na infraestrutura do sistema, visando o encaminhamento adequado dos pacotes entre as *subnets* existentes na Prefeitura da Estância Turística de São Roque e fora dela.

Isaías Gomes dos Santos
Diretor de Informática
RG: 45.127.633-4

2.8.5. Hospedagem

a. A **SFP** deverá permitir e possuir estrutura para montagem de um servidor WEB com hospedagem de sites, podendo o servidor ser o Apache ou o IIS.

2.9. Monitoramento

2.9.1. Introdução ao Sistema de Monitoramento

A **Solução de Firewall/Proxy (SFP)** deverá possuir monitoramento em tempo real para os recursos e serviços relacionados abaixo e que nela estejam em funcionamento.

2.9.2. Monitoramento de Navegação

a. Usuários navegando em *sites* da Internet;
b. Endereços IP das estações conectadas à Internet;
c. *Sites* que estão sendo acessados e quem os está acessando de forma específica;
d. Requisições de acesso que foram negadas pelo serviço/servidor de *proxy*.

2.9.3. Monitoramento de Rede

a. Tráfego de dados de forma individual por *interface*;
b. Protocolos que estão sendo utilizados individualmente;
c. Portas em uso nas conexões;
d. Endereços IP em tráfegos de rede.

2.9.4. Monitoramento de VPN

a. *Status* das conexões VPN;
b. Tipos de acessos VPN em uso no momento;
c. VPN individual;
d. VPN com conexão via SSL;
e. Conexão de VPN que estão abertas.

2.9.5. Monitoramento de *Links*

a. Estado dos *links* de dados;
b. *Status* dos pacotes em passagem nas *interfaces* de rede;
c. Demonstrar os pacotes que foram perdidos na conexão.

2.10. Autenticação

2.10.1. Introdução às Autenticações Suportadas

Para acesso à base de mensagens do servidor de navegação na Internet, entre outros serviços já mencionados, a **Solução de Firewall/Proxy (SFP)**, além de possuir uma base de dados de usuários interna, deverá também dar suporte a outros protocolos de autenticação integrada. Sendo estes relacionados abaixo.

Isaías Gomes dos Santos
Diretor de Informática
RG: 45.127.633-4

2.10.2. Protocolos para Autenticação Integrada

a. LDAP;
b. MSNT;
c. NTLM;
d. PAM;
e. SMB AUTH.

2.11. Relatórios

2.11.1. Introdução aos Relatórios a Serem Emitidos

A **Solução de Firewall/Proxy (SFP)** deverá emitir e armazenar relatórios dos recursos e serviços em funcionamento nos sistemas conforme relação abaixo.

2.11.2. Relatórios de Navegação

a. Relatórios dos acessos diários de cada usuário;
b. Relatórios de acesso mensal de cada usuário;
c. Os *sites* da Internet que foram acessados pelos usuários;
d. Estatísticas de acesso;
e. Quantidade (em *bytes*) de conteúdo baixado;
f. A porcentagem de utilização do recurso por usuário;
g. Tempo utilizado da navegação realizada por cada usuário;
h. Permitir que sejam realizados filtros de buscas considerando a data e horário das ações;
i. Permitir a impressão dos relatórios emitidos e armazenados.

2.11.3. Relatórios de Conexão VPN

a. Realizar a emissão dos relatórios de forma individual por conta de VPN existente;
b. Permitir que sejam aplicados filtros de buscas no serviço de VPN;
c. Emitir relatórios de auditorias das conexões VPN, sendo estas dos tipos SSL, *Open* VPN e IPSEC;
d. Relatório do tráfego de dados por conexão, considerando a quantidade de *bytes* enviados/e recebidos;
e. Relatório tempo total em que uma conexão VPN está aberta e estabelecida;
f. Relatório das ações realizadas sobre as conexões – se conectado ou desconectado;
g. Permitir a impressão dos relatórios referentes às conexões VPN.

2.11.4. Relatórios Gerais Referentes à Suporte Técnico

a. Emitir relatório dos LOGs das modificações realizadas pelo administrador do sistema em todas as estruturas do servidor;
b. Permitir que sejam realizados filtros de busca dos relatórios que se queira emitir;
c. Relatório das ações realizadas pela equipe técnica de suporte à **SFP**;
d. Permitir a impressão de todos os relatórios referentes às intervenções no servidor.

Isaías Gomes dos Santos
Diretor de Informática
RG: 45.127.633-4

2.12. Relatórios Gráficos

2.12.1. Introdução aos Relatórios Gráficos

Visando facilitar o trabalho de auditoria e monitoramento, a **Solução de Firewall/Proxy (SFP)** deve possuir a funcionalidade de emissão de relatórios gráficos dos itens abaixo relacionados.

2.12.2. De uso do Processador

a. Emitir relatórios gráficos da carga média do processamento utilizado;
b. Emitir relatório gráfico da utilização do processador como um todo;
c. Emitir relatório gráfico da temperatura do processador.

2.12.3. De utilização da Memória

a. Emitir relatório de utilização da memória RAM e memória SWAP (se possuir).

2.12.4. De uso do Disco Rígido (HD)

a. Emitir relatório gráfico de utilização do disco rígido (HD);
b. Emitir relatório gráfico da performance do disco rígido (HD);
c. Emitir relatório gráfico da temperatura do disco rígido (HD).

2.12.5. De tráfego nas *Interfaces*

a. Emitir relatório gráfico de taxa de transferência de entrada e saída (*input/output*) das *interfaces* de rede;
b. Emitir relatório gráfico da utilização das liberações de entrada e liberações de saída.

2.12.6. Do Sistema

a. Emitir relatório gráfico sobre a performance dos *coolers* do *hardware* do servidor;
b. Emitir relatórios gráficos dos processos ativos no sistema;
c. Emitir relatórios gráficos do tempo de atividade do sistema;

2.12.7. Armazenamento dos Gráficos

a. Visando possíveis auditorias e eventuais consultas, o **SFP** deverá armazenar os LOGs dos gráficos por um período mínimo de 04 (quatro) anos.

2.13. Atualizações

2.13.1. Introdução às Rotinas de Atualização

Visando segurança em toda a infraestrutura da **Solução de Firewall/Proxy (SFP)** a ser contratada pela Prefeitura da Estância Turística de São Roque, deverão ser disponibilizadas atualizações de correções de falhas, bem como de versões sempre que houver necessidade julgada, e de pacotes disponibilizados pela empresa desenvolvedora. Isto, tanto para a ferramenta completa como para os pacotes de serviços individuais da mesma.

2.13.2. Do Sistema

a. O desenvolvedor da **SFP** deverá disponibilizar diariamente atualizações para a base de dados da solução. Nesta rotina, os itens a serem contemplados deverão envolver sites im

Isaias Gomes dos Santos
Diretor de Informática
RG: 45.127.633-4

divididos por categorias, base de assinaturas de ataques, protocolos e correções de segurança da solução;

b. Quanto as atualizações de *upgrade* de novas versões das ferramentas e serviços ou **SFP** como um todo, deverá ser previamente agendada com o Departamento de Informática da Prefeitura da Estância Turística de São Roque. Sendo que esta deverá ser realizada com acompanhamento técnico e poderá ser realizada *in loco* ou remotamente;

2.13.3. Da Solução Antivírus

a. As atualizações destinadas ao antivírus da **SFP** deverão ser realizadas de forma automática diariamente conforme disponibilização de pacotes por parte do desenvolvedor.

3. Garantia

3.1. Introdução à Garantia

Visando a transparência e certeza de qualidade da **Solução de Firewall/Proxy (SFP)**, deverá ser dada garantia de bom funcionamento de toda a aplicação.

3.2. Compreensão da Garantia

a. A garantia da licença deverá cobrir todo o período da contratação;
b. A empresa ofertante da **SFP** deverá ser oficialmente credenciada pelo desenvolvedor ou seu representante no Brasil;
c. Toda a cobertura de garantia deverá ser sem custo nenhum para a Prefeitura da Estância Turística de São Roque.

4. Treinamento e Implantação

4.1. Introdução às necessidades de Treinamento e Implantação

Visando familiarização e utilização de toda a estrutura da **Solução de Firewall/Proxy (SFP)**, a empresa vencedora do processo deverá realizar o treinamento aos colaboradores do Departamento de Informática da Prefeitura da Estância Turística de São Roque e realizar a implantação de toda a ferramenta.

4.2. Treinamento

a. O treinamento deverá ser realizado nas instalações da Prefeitura da Estância Turística de São Roque;
b. Para até 05 (cinco) colaboradores do Departamento de Informática;
c. Deverá ocorrer no prazo máximo de 15 (quinze) dias após a assinatura do contrato;
d. Deverão ser abordados assuntos como: instalação completa da **SFP**, configuração e uso de todos os recursos citados neste Descritivo Técnico.
e. Deverá ser utilizado material oficial relativo à instalação, configuração, uso e monitoramento da ferramenta, devendo cobrir todas suas funcionalidades;

Isaías Gomes dos Santos
Diretor de Informática
RG: 45.127.633-4

f. Deverão ser entregues manuais completos da **SFP** no formato impresso e digital (PDF ou DOC) até o dia do treinamento. Estes deverão estar nos idiomas português do Brasil ou inglês.
g. O treinamento deverá ser ministrado em português brasileiro.

4.3. Implantação da Solução

a. A implantação e instalação iniciarão imediatamente após a assinatura do contrato e do recebimento da ordem de serviço emitido pelo Departamento de Informática da Prefeitura da Estância Turística de São Roque;
b. No período de até 10 (dez) dias após a emissão da ordem de serviço deverá ocorrer a entrega da documentação de licenciamento da **SFP**;
c. A implantação deverá ser realizada *in loco* nas dependências da Prefeitura da Estância Turística de São Roque, sendo acompanhada pelos técnicos do Departamento de Informática;
d. A conclusão da implantação deverá se dar em até 15 (quinze) dias corridos após a disponibilização do *hardware* pela Prefeitura da Estância Turística de São Roque;
e. Deverá ser realizada a importação das credenciais de acesso à Internet do servidor *Proxy* (*Squid*) atualmente em uso pela Prefeitura da Estância Turística de São Roque, bem como a importação/reelaboração das regras indicadas pelos técnicos do Departamento de Informática que acompanharão a implantação;
f. Deverão ser importadas/reelaboradas as regras do *firewall* (*SuSEfirewall / IPTables*) atualmente em uso conforme indicação dos técnicos do Departamento de Informática que acompanharão a implantação da solução;
g. Após a implantação da **SFP**, será celebrado Termo de Conclusão de Projeto de Implantação que deve ser apresentado pela contratada;
h. A versão do produto/solução a ser instalada deverá ser a mais recente (excluindo verões betas e de teste) disponibilizada pelo desenvolvedor.

5. Suporte, Manutenção e SLA

5.1. Introdução aos Serviços a Serem Prestados

Visando continuidade dos serviços da **Solução de Firewall/Proxy (SFP)**, deverá haver disponibilidade de suporte técnico completo da ferramenta à equipe do Departamento de Informática da Prefeitura da Estância Turística de São Roque sempre que necessário, conforme consta neste Descritivo Técnico.

5.2. Prestação de Serviço

a. A equipe de suporte da **SFP** deverá estar à disposição em regime 9x7 – de segunda a sexta – das 08h às 18h (horário comercial);
b. Para abertura de chamado, deverão ser disponibilizados canais de atendimento por telefone, *e-mail*, sistema ou *chat online*; sendo que estes devem ser previamente indicados pelo

Isaías Gomes dos Santos
Diretor de Informática
RG: 45.127.533-4

desenvolvedor/representante. Em caso de telefone, deverá ser disponibilizada uma Central de Atendimento no Brasil.

c. Deve haver disponibilidade para abertura de chamados de manutenção de 24 (vinte e quatro) horas por dia nos 7 (sete) dias da semana através dos canais via Internet (*online*);
d. O atendimento deve ser realizado em português (Brasil).
e. A solução proposta deverá ser atualizada sem custo adicional durante o período de vigência do contrato, inclusive em caso de *upgrade* de versão conforme item **2.13** deste Descritivo Técnico;
f. O SLA (*Service Level Agreement*) para solução de problemas da **SFP** não deverá ultrapassar 48 (quarenta e oito) horas a partir da abertura do chamado; sendo que em 12 (doze) horas deverá ser para tempo de resposta e 36 (trinta e seis) horas para resolução efetiva do problema;
g. Todo o chamado aberto junto ao desenvolvedor da **SFP** deverá ser devidamente registrado e vinculado a um número de protocolo e ser informado ao usuário solicitante que venha a representar a Prefeitura da Estância Turística de São Roque na ação;
h. Deverá ser mantido um histórico de todo o atendimento prestado para eventuais consultas.

Isaías Gomes dos Santos
Diretor de Informática
RG: 45.127.633-4

PREFEITURA DA ESTÂNCIA TURISTICA DE SÃO ROQUE
DEPARTAMENTO DE ADMINISTRAÇÃO

Divisão de Compras e Licitações

Orçamento Nº 952.2017

PROPOSTA COMERCIAL	
Fornecedor: NETDEEP TECNOLOGIA LTDA. ME.	
CNPJ: 11.282.095/0001-08	
Endereço/ CEP: RUA QUATRO, 958 – CENTRO – ORLANDIA – SP – CEP: 14620-000	
Fone / Fax: 16-3726-3961	**E-mail: comercial@netdeep.com.br**
Nota Fiscal Eletrônica: Sim (x) Não ( )	**Nota Fiscal de: Consumo/ Venda ( ) Serviço (x)**

Solicito cotação dos itens abaixo:

Item	Qtde	Unid. Med.	Especificação do Material	Marca/ Modelo	P. Unitário	P. Total
001	1	Serviço	Contratação de Solução de Firewall e Proxy Completa com implantação, Treinamento, suporte, manutenção e consultoria em segurança de Redes. **- Especificação Técnica no Anexo 2.**		R$ 6.100,00	R$ 6.100,00

TOTAL DO ORÇAMENTO:	R$ 6.100,00

Prazo da Proposta: 30 dias	**Condição (Dias) de Pagamento: 28 dias**	
Entrega: Sim (x) Não ( )	**Condição de Entrega: 10 dias**	
Faturamento Mínimo: R$	**Frete: Sim ( ) Não (x)**	**Valor: R$**

Nome do Responsável (CAMPO OBRIGATÓRIO)	**Assinatura e Carimbo (CAMPO OBRIGATÓRIO)**
_____ANDRE LUIZ RODRIGUES FERREIRA_____	11.282.095/0001-08 NETDEEP TECNOLOGIA LTDA - ME RUA QUATRO N.º 958 CENTRO - CEP 14.620-000 ORLÂNDIA - SP

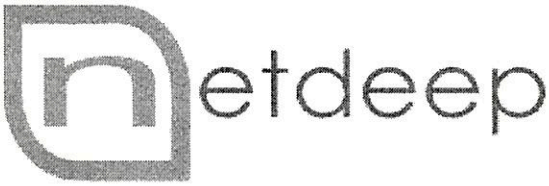
CONTATO
Jéssica Zacante ☎ Fone: 11 4784-9682 🖷 Fax: 4712-4024 ✉ E-mail: jznascimento@saoroque.sp.gov.br

Protocolo ICMS 42/09, atualizado pelo protocolo ICMS 85/10:

Cláusula segunda *Ficam obrigados a emitir Nota Fiscal Eletrônica – NF-e, modelo 55, em substituição à Nota Fiscal, modelo 1 ou 1-A, a partir de 1º de dezembro de 2010, os contribuintes que, independentemente da atividade econômica exercida, realizem operações:*

I - destinados à Administração Pública direta ou indireta, inclusive empresa pública e sociedade de economia mista, de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios; (...).

PROPOSTA COMERCIAL



NETDEEP SECURE 3

NEXT GENERATION OPEN SOURCE FIREWALL

Projeto elaborado para: **PREFEITURA MUNICIPAL DE SÃO ROQUE**

Projeto elaborado por: **André Ferreira**

Título do projeto: **Netdeep Secure**

Data: **30/01/2017**

Validada Proposta: **60 dias**

CONTEÚDO CONFIDENCIAL

O CONTEÚDO DESTA PROPOSTA SUBSTITUI INTEGRALMENTE TODA E QUALQUER PROPOSTA ENVIADA ANTERIORMENTE

Descrição do projeto

Tecnologia e Segurança em Profundidade

O **Netdeep Secure** é uma solução de acesso seguro a Internet. É um firewall que provê praticamente todas as funcionalidades de segurança de rede que uma empresa pode precisar. São sistemas simples de instalar e fáceis de manter, oferecendo uma excepcional relação de custo-benefício e um desempenho excelente.

Utiliza a tecnologia **DPI (Deep Packet Inspection)** para realizar vários tipos de filtros Web, garantindo uma melhor performance da rede, permitindo que os usuários utilizem o serviço de forma eficiente e segura, proporcionando um controle minucioso da utilização do serviço de acesso a Web, bloqueando sites indesejados, Malwares, SPAMS e tentativas de invasão. Ele permite detectar e bloquear mais de 10.00 ataques remotos e a criação de assinaturas personalizadas para detecção de novas ameaças (zero day). Por ser parte do próprio sistema operacional, possui excelente desempenho e suporte a um fluxo intenso de dados, proporciona um registro detalhado das tentativas de violação das regras de segurança e tentativas de invasão. Estes dados podem contribuir significativamente para a definição de novas medidas de proteção. A administração pode ser feita remotamente de forma fácil e segura.

Funcionalidades:

Firewall de Aplicação

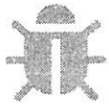
Oferece proteção em 7 camadas, inspecionando **(Deep Packet Inspection)** pacotes e tráfego de dados baseado nas características de cada aplicação, nas informações associadas a todas as camadas, inclusive inspeção de tráfego SSL.

Controle Web

Através de vários filtros, você pode definir uma política de acesso à Internet, por sites, categorias (ex: sites pornográficos, redes sociais, jogos, etc) por usuário, endereço IP, ou grupos.

Conexão segura por VPN

Conecte escritórios e usuários remotos com segurança, integrando e reduzindo custos com comunicação.



Antivírus

Fique livre das ameaças que chegam pela Internet. Possuímos 2 motores de antivírus (ESET e Clamav) que garantem que seus computadores fiquem limpos.

Detecção e Prevenção de Intrusos

Proteja seus servidores e estações de invasores. Contamos com um banco de dados para detecção de milhares de ataques direcionados e ameaças persistentes (APT).

netdeep

TECNOLOGIA E SEGURANÇA EM PROFUNDIDADE

DHCP e DNS

Serviços de DHCP, DNS e DNS dinâmico que facilitam a vida do administrador da rede.

Controle de banda e tráfego

Defina o consumo da banda de seu link de Internet, controlando por horário, usuário, protocolo ou aplicativo.

Relatórios e auditoria

Obtenha relatórios completos e personalizados de navegação filtrados por data, horário, usuário, endereço IP, URL ou domínio com exportação para Excel. Saiba se os colaboradores de sua empresa estão de acordo com a política definida pelo departamento de TI.

Redundância e Balanceamento

Garantimos que a sua empresa fique todo tempo online. Você pode dividir a banda por links de conexão diferentes (balanceamento) ou ter uma contingência.

Alta-disponibilidade

Sabemos que o seu negócio não pode parar. Com este recurso, você tem um cluster ativo-passivo, que garante redundância de hardware.

Filtro transparente HTTP e HTTPS

Filtro de conteúdo web transparente que anula a necessidade de configurações manuais nas estações, com inspeção de tráfego criptografado.

Autenticação Centralizada

Centralizamos a autenticação com serviços de diretório como Active Directory e LDAP, com transparência e single sign-on

Wifi e Captive Portal

Gerencie os usuários externos que se conectam em sua rede wireless, autenticando-os através de um portal.

Dashboard

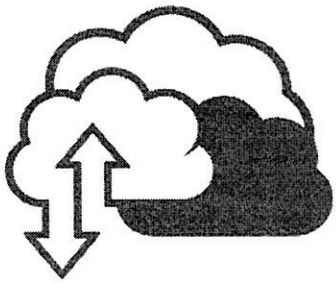
Estatísticas precisas do tráfego e consumo de recursos de seu firewall através de alguns cliques.

Safe Search

Bloqueie conteúdo impróprio (ex: imagens pornográficas) em sites de busca como Google, Bing e Yahoo.

Rua 4 (Quatro), 958 – Centro – Orlândia – SP | 14620-000 | (16) 3726-3961 – comercial@netdeep.com.br

Netdeep Secure Network



Com o rápido desenvolvimento da tecnologia da informação e a maior penetração da Internet junto à população, o número de ameaças às quais os usuários de computadores estão sujeitos cresce proporcionalmente. Portanto, a proteção efetiva consiste em diferentes componentes e tecnologias de proteção que trabalham em cooperação.

Uma dessas tecnologias de proteção é o Netdeep Secure Network. A través da parceria com diversos fabricantes e desenvolvimento interno criamos uma rede de segurança especial que permite que os usuários obtenham:

- Nível de proteção adicional pela integração entre os módulos do firewall
- Dados de reputação de URL e domínios
- Reação rápida a novas ameaças.

Assinatura

Disponível em 5 versões de assinaturas: **START, BASIC, STANDARD, PROFESSIONAL, ENTERPRISE** com níveis de funcionalidades e suporte técnico explicados a seguir:

	FUNCIONALIDADES					
		START	**BASIC**	**STANDARD**	**PROFESSIONAL**	**ENTERPRISE**
1	Firewall de aplicação	✔	✔	✔	✔	✔
2	Regras por Zonas (Local, Internet, Wifi, DMZ)	✔	✔	✔	✔	✔
3	Inspeção profunda de pacotes (DPI)	✔	✔	✔	✔	✔
4	Proxy Web	✔	✔	✔	✔	✔
5	Filtro de URL	✔	✔	✔	✔	✔
6	Autenticação local, Radius, LDAP ou Active Directory	✔	✔	✔	✔	✔
7	Políticas de acesso web por grupos	✔	✔	✔	✔	✔
8	Relatórios de navegação	✔	✔	✔	✔	✔

9	DNS dinâmico	✔	✔	✔	✔	✔
10	Servidor DHCP	✔	✔	✔	✔	✔
11	Captive Portal e gestão Wifi	✔	✔	✔	✔	✔
12	Antivírus Clamav	✔	✔	✔	✔	✔
13	Dashboard de monitoramento	✔	✔	✔	✔	✔
14	SafeSearch	✔	✔	✔	✔	✔
15	SNMP	✔	✔	✔	✔	✔
16	VPN SSL	✔	✔	✔	✔	✔
17	VPN IPSec	✔	✔	✔	✔	✔
18	Monitor de Consumo de banda em tempo real	✔	✔	✔	✔	✔
19	Servidor Radius			✔	✔	✔
20	Controle de banda			✔	✔	✔
21	Servidor DNS			✔	✔	✔
22	Roteamento estático e por origem			✔	✔	✔
23	Detecção e Prevenção de Intrusos			✔	✔	✔
24	Redundância de conexão com a Internet			✔	✔	✔
25	Balanceamento de conexão com a Internet			✔	✔	✔
26	Inspeção SSL				✔	✔
27	Alta-disponibilidade				✔	✔

28	Antivírus ESET Professional					✓
	SERVIÇOS					
		START	**BASIC**	**STANDARD**	**PROFESSIONAL**	**ENTERPRISE**
29	Documentação	✓	✓	✓	✓	✓
30	Atualizações/upgrades	✓	✓	✓	✓	✓
31	Treinamento online		✓	✓	✓	✓
32	Netdeep Secure Network			✓	✓	✓
33	Instalação/configuração/ migração		✓	✓	✓	✓
34	Suporte técnico nível 1		✓	✓	✓	✓
35	Suporte técnico nível 2				✓	✓
36	Gerenciamento e Monitoramento (Firewall, Antivírus e Backup)					✓
37	Assinatura	**Grátis**	**Anual/Mensal**	**Anual/Mensal**	**Anual/Mensal**	**Anual/Mensal**
38	Licenciamento	**Ilimitado**	**Usuário/host**	**Usuário/host**	**Usuário/host**	**Usuário/host**

Nível de Atendimento e suporte técnico

Suporte técnico – Nível 1: para resolução de dúvidas, através de sistema de chamados, com tempo de resposta de 8 horas e interação por telefone, e-mail ou chat.

Suporte técnico – Nível 2: para resolução de problemas, através de sistema de chamados, com tempo de resposta de 4 horas e interação por telefone, e-mail ou chat, **com acesso remoto ou visita presencial** de nossos analistas.

Equipe envolvida no projeto:

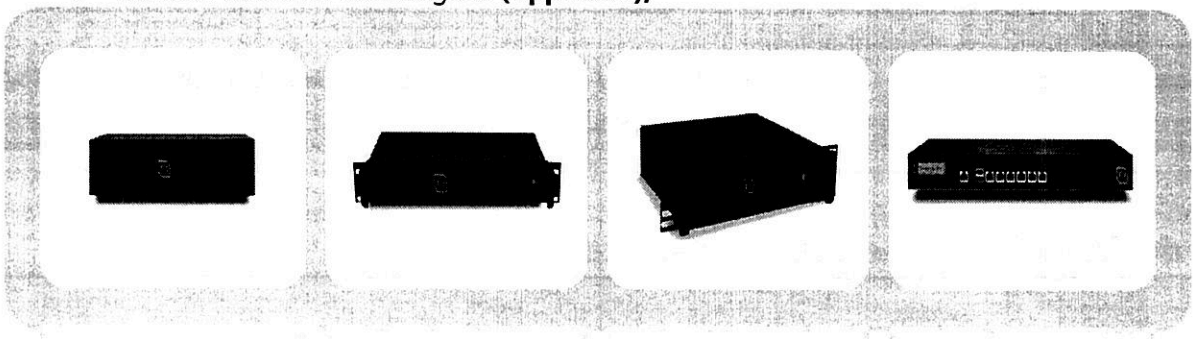
O nosso foco é possuir soluções e serviços para diminuir os riscos do negócio de nossos clientes e prover soluções que aumentem a sua produtividade. No perfil típico dos profissionais da Netdeep estão as seguintes soluções:

Gerência de TI	Suporte Técnico e Infraestrutura	Segurança da Informação
• Práticas de governança de TI baseado em ITIL • Inventário de Hardware e Software • Análise de Produtividade dos usuários • Análise de Performance de servidores e estações • Hardening de Segurança de estações e servidores • Recuperação de desastres • Controle Remoto Corporativo	• Sistemas operacionais Windows, Linux e Unix • Serviços de Internet (Web, E-mail, FTP) • Servidores de arquivos e impressão • Clustering e Alta-disponibilidade • Servidores de Terminal e aplicação • Gerenciamento de banco de dados	• Política de Segurança • Segurança de Perímetros • Antívirus, Firewall, Proxy e Filtro de Conteúdo • Virtual Private Network • Correlação de eventos de segurança por análise forense • Sistemas de Detecção e Prevenção de Intrusos • Gerenciamento unificado de ameaças (UTM) • Antispam e segurança de servidores de e-mail • Análise de vulnerabilidades, pentest e malwares.

Distribuição

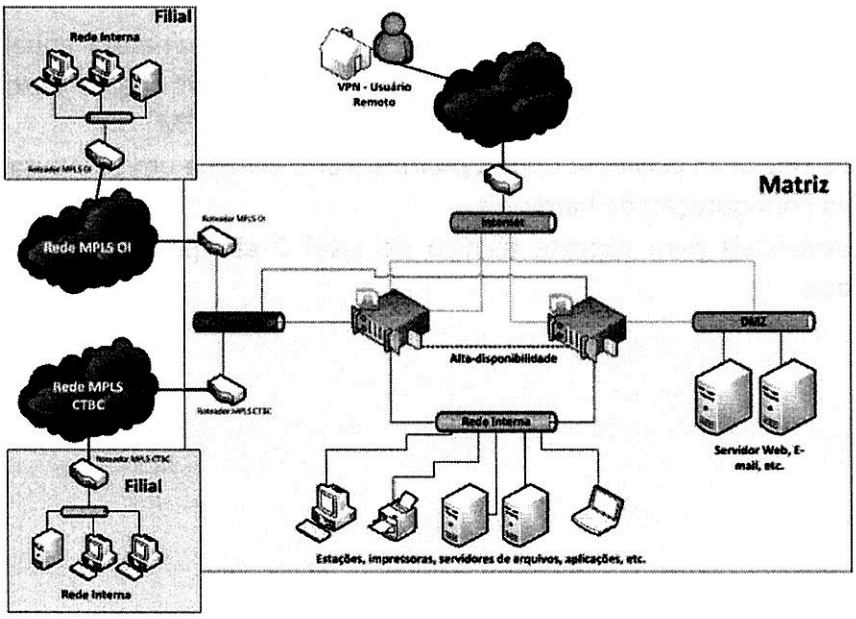
O sistema pode ser executado em uma das plataformas abaixo:

- Ambiente virtualizado (Vmware, Hyper-V, Xen, Virtual Box)
- Servidor dedicado fornecido pelo cliente
- Servidor dedicado homologado **(Appliance),**



NDS-30	NDS-60	NDS-100	NDS-300
Até 50 usuários	**Até 60 usuários**	**+100 usuários**	**+300 usuários**
Mini-PC	**Para rack, 1U**	**Para rack, 2U**	**Para rack, 1U**
Processador Intel	**Processador Intel**	**Processador Intel**	**Processador Intel**
2Gb de RAM	**4 Gb de RAM**	**8 Gb de RAM**	**12 Gb de RAM**
HD 500 GB	**HD 500 GB**	**HD +500 GB**	**SSD +300 GB**
3 placas de rede	**3-5 placas de rede**	**3-5 placas de rede**	**5-8 placas de rede**

Diagrama de Rede Suportado



Investimento

Item	Descrição	Unitário	Qtde.	Total Anual
01	**Assinatura – 12 Meses – Firewall Netdeep Secure PROFESSIONAL – 300 usr**	R$ 6.100,00	01	**R$ 6.100,00**
			Total Anual	**R$ 6.100,00**

Condições de Fornecimento

Prazo de pagamento: 30 dias
Forma de pagamento: Boleto ou depósito bancário

Prazo de entrega/execução do projeto

15 dias;

Tarifas, impostos e taxas especiais

Todas as taxas, tarifas ou impostos incidentes aos serviços listados no presente documento de Declaração de Trabalho estão incluídos neste preço.

Despesas

As despesas de viagem tais como: frete, transporte aéreo e terrestre, hospedagem, refeições e hora técnica (implantação e suporte presencial) são de responsabilidade da PREFEITURA MUNICIPAL DE SÃO ROQUE.

Notas

- Para obter a continuidade dos serviços contemplados na assinatura anual é necessária a sua renovação anual. Será concedido um desconto no preço em vigor. Caso faça a opção pela assinatura mensal, sofrerá reajuste anual baseado no índice IGPM
- O Appliance é opcional. O cliente pode optar instalar o sistema um computador (físico ou virtual) com a mesma configuração de hardware.
- As visitas presenciais para suporte técnico de nível 2 são previamente agendadas conforme disponibilidade.

Contrato de Conformidade

As assinaturas abaixo indicam a concordância do CLIENTE e da NETDEEP para os produtos, pressupostos, estimativas de faturamento e despesas, conforme documentados nesta declaração de trabalho.

CLIENTE	NETDEEP
Razão Social:	Nome: NETDEEP TECNOLOGIA LTDA.
CNPJ:	CNPJ: 11.282.095/0001-08
Endereço:	Endereço: RUA 04, 958 – CENTRO – ORLANDIA – SP – CEP: 14620-000
Nome do Responsável:	Nome do Responsável: ANDRÉ LUIZ RODRIGUES FERREIRA
Cargo:	Cargo: DIRETOR
Data:	Data:
Assinatura:	Assinatura:

Este acordo deve ser regido pelas leis brasileiras, sendo eleito o Fórum da Comarca de Orlândia.
Seguimos a disposição.

Atenciosamente,

André Luiz Rodrigues Ferreira
Netdeep Tecnologia

Receita Federal PGFN **CERTIDÃO**

MINISTÉRIO DA FAZENDA
Secretaria da Receita Federal do Brasil
Procuradoria-Geral da Fazenda Nacional

CERTIDÃO NEGATIVA DE DÉBITOS RELATIVOS AOS TRIBUTOS FEDERAIS E À DÍVIDA ATIVA DA UNIÃO

Nome: NETDEEP TECNOLOGIA LTDA - ME
CNPJ: 11.282.095/0001-08

Ressalvado o direito de a Fazenda Nacional cobrar e inscrever quaisquer dívidas de responsabilidade do sujeito passivo acima identificado que vierem a ser apuradas, é certificado que não constam pendências em seu nome, relativas a créditos tributários administrados pela Secretaria da Receita Federal do Brasil (RFB) e a inscrições em Dívida Ativa da União (DAU) junto à Procuradoria-Geral da Fazenda Nacional (PGFN).

Esta certidão é válida para o estabelecimento matriz e suas filiais e, no caso de ente federativo, para todos os órgãos e fundos públicos da administração direta a ele vinculados. Refere-se à situação do sujeito passivo no âmbito da RFB e da PGFN e abrange inclusive as contribuições sociais previstas nas alíneas 'a' a 'd' do parágrafo único do art. 11 da Lei nº 8.212, de 24 de julho de 1991.

A aceitação desta certidão está condicionada à verificação de sua autenticidade na Internet, nos endereços <http://rfb.gov.br> ou <http://www.pgfn.gov.br>.

Certidão emitida gratuitamente com base na Portaria Conjunta RFB/PGFN nº 1.751, de 2/10/2014.
Emitida às 16:10:59 do dia 11/12/2017 <hora e data de Brasília>.
Válida até 09/06/2018.
Código de controle da certidão: **799C.098A.7A3A.7A70**
Qualquer rasura ou emenda invalidará este documento.

Nova Consulta Preparar página para impressão

PREFEITURA DA ESTÂNCIA TURISTICA DE SÃO ROQUE
DEPARTAMENTO DE ADMINISTRAÇÃO

Divisão de Compras e Licitações

Orçamento Nº 952.2017

PROPOSTA COMERCIAL	
Fornecedor: ALLCOMNET TECNOLOGIA E SISTEMAS – EPP – EIRELI	
CNPJ:04.44.094/0001-87	
Endereço/ CEP:RUA SANTO ANTONIO, 43 – 4 AND. – CONJ 401 – JD SÃO PAULO – CEP 07110-150	
Fone / Fax (011) 2626-7130	**E-mail: rogerio.prenholato@allcomnet.com.br**
Nota Fiscal Eletrônica: Sim (X) Não ( )	**Nota Fiscal de: Consumo/ Venda (X) Serviço ( )**

Solicito cotação dos itens abaixo:

Item	Qtde	Unid. Med.	Especificação do Material	Marca/ Modelo	P. Unitário	P. Total
001	1	Serviço	Contratação de Solução de Firewall e Proxy Completa, WatchGuard Firebox M300 Series Hardware e WatchGuard Firebox M300 with 1-yr Basic Security Suite, com implantação, Treinamento, suporte, manutenção e consultoria em segurança de Redes. De acordo com seu descritivo técnico. **- Especificação Técnica no Anexo 2.**	WATCHGUARD FIREBOX M300	23.000,00	23.000,00

TOTAL DO ORÇAMENTO:	**R$ 23.000,00**

Prazo da Proposta: 30 DIAS	**Condição (Dias) de Pagamento: 28 DIAS**	
Entrega: Sim (X) Não ( )	**Condição de Entrega: 10 DIAS**	
Faturamento Mínimo: R$ -X-	**Frete: Sim ( ) Não (X)**	**Valor: R$ -X-**

Nome do Responsável (CAMPO OBRIGATÓRIO)

Assinatura e Carimbo (CAMPO OBRIGATÓRIO)

04.424.094/0001-87
ALLCOMNET
TECNOLOGIA E SISTEMAS EIRELI - EPP
Rua Santo Antonio, 43 - 4º Andar Cj. 401 Ed. CII
Centro - CEP 07110-150
Guarulhos - SP.

CONTATO

Jéssica Zacante ☎ Fone: 11 4784-9682 🖷 Fax: 4712-4024 ✉ E-mail: jznascimento@saoroque.sp.gov.br

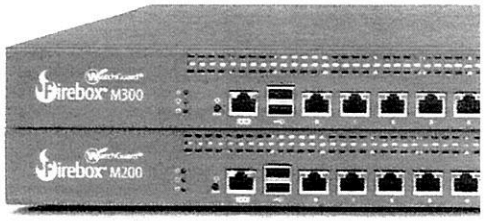
Protocolo ICMS 42/09, atualizado pelo protocolo ICMS 85/10:

Cláusula segunda *Ficam obrigados a emitir Nota Fiscal Eletrônica – NF-e, modelo 55, em substituição à Nota Fiscal, modelo 1 ou 1-A, a partir de 1º de dezembro de 2010, os contribuintes que, independentemente da atividade econômica exercida, realizem operações:*
I - destinados à Administração Pública direta ou indireta, inclusive empresa pública e sociedade de economia mista, de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios; (...).

DATASHEET

Firebox M200 e M300

Capacidade de processamento do firewall de até 4 Gbps e do UTM de 800 Mbps
Até 75 VPNs de filiais de escritório, 100 VPNs para dispositivos móveis e 200 VLANs



SEGURANÇA DE GRAU CORPORATIVO PARA EMPRESAS DE PEQUENO E MÉDIO PORTE

Como as empresas menores são geralmente menos protegidas e mais suscetíveis a invasões, as pequenas empresas se tornaram um grande alvo para ataques cibernéticos. Os firewalls do Firebox® M200 e M300 são especialmente projetados para defender todos os tipos de empresas pequenas contra ataques que não são menos ameaçadores que aqueles contra corporações maiores. Nossa arquitetura de produtos exclusiva permite que pequenas e médias empresas avaliem os melhores serviços de segurança — desde filtragem de URL até controle de aplicativos e prevenção contra perda de dados, sem os custos e as complexidades de várias soluções pontuais. O M200 e o M300 fazem parte da plataforma de segurança premiada da WatchGuard, Firebox. A plataforma não só fornece o conjunto mais completo de controles de segurança unificados no mercado de hoje em dia, mas foi a primeira a oferecer soluções de forma consistente para lidar com ameaças de rede novas e em evolução, incluindo ransomware e malwares avançados.

> "Os resultados dos testes demonstraram que o Firebox M300 teve um desempenho mais rápido do que soluções de UTM concorrentes com recursos de UTM padrão ativados em fluxos de dados criptografados e não criptografados. A solução da WatchGuard fornece serviços de segurança de primeira classe para defender pequenas e médias empresas contra conteúdos maliciosos com uma proteção de firewall eficaz."
>
> *~ Teste de desempenho da Miercom*

DESEMPENHO VELOZ

As soluções de gerenciamento unificado de ameaças (UTM) do Firebox M200 e M300 são até 218% mais rápidas do que produtos concorrentes com todas as camadas de segurança ativadas e até 385% mais rápidas ao realizar inspeção de HTTPS, segundo o laboratório de testes independentes Miercom. Isto garante que você nunca tenha que comprometer a segurança de rede pelo desempenho.

IMPLEMENTAÇÃO SIMPLES E RÁPIDA

As pequenas e médias empresas têm equipes menores e menos técnicas, o que pode tornar a expansão de rede um desafio. RapidDeploy – uma ferramenta poderosa de configuração e implementação com base em nuvem — é padrão nos aparelhos Firebox da WatchGuard. Com ela, a equipe de TI pode criar e armazenar dados de configuração na nuvem – pública ou privada – e enviar o dispositivo diretamente ao seu destino. Quando o dispositivo chega, ele pode ser conectado à nuvem para fazer download das configurações, economizando dinheiro e tempo de viagem da equipe.

FÁCIL DE GERENCIAR E ENTENDER

Os aparelhos M200 e M300 não só são fáceis de configurar e implementar, como também são projetados com ênfase no gerenciamento centralizado, tornando o gerenciamento de rede e de políticas simples e direto. O WatchGuard Dimension, incluso na compra, fornece um conjunto de visibilidade de big data e ferramentas de geração de relatórios que identificam instantaneamente e retificam ameaças de segurança de rede, problemas e tendências para que você possa tomar uma ação corretiva ou preventiva imediata. A segurança é complexa, mas a execução não precisa ser.

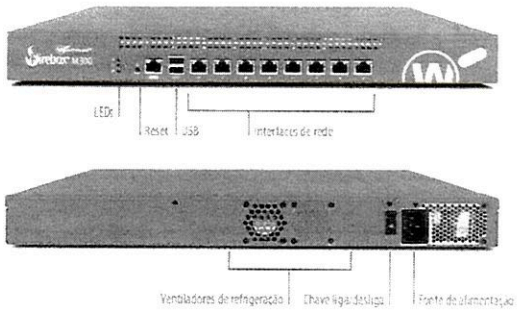
RECURSOS E BENEFÍCIOS

- Portas Ethernet Gigabit oferecem compatibilidade com infraestruturas de backbone de LAN de alta velocidade e conexões WAN gigabit.
- Os processadores de vários núcleos Freescale de última geração fornecem o poder de executar todos os mecanismos de verificação de segurança em paralelo sem causar gargalos de desempenho.
- Nada consegue ser mais fácil do que a configuração do tipo "arrastar e soltar" para VPNs de filiais da WatchGuard – bastam três cliques para conectar o seu escritório remoto.
- Relatórios de conformidade integrados, incluindo PCI e HIPAA, significam acesso de um clique aos dados de que você precisa para garantir que os requisitos de concordância sejam atendidos.
- Capacidade de processamento do firewall de até 4 Gbps. Mesmo com os serviços de segurança adicionais ativados, ainda há uma capacidade de processamento de 800 Mbps.

Firebox	M200	M300
CAPACIDADE DE PROCESSAMENTO		
Capacidade de processamento do firewall	3,2 Gbps	4,0 Gbps
Capacidade de processamento da VPN	1,2 Gbps	2 Gbps
Capacidade de processamento do AV	620 Mbps	1,2 Gbps
Capacidade de processamento do IPS	1,4 Gbps	2,5 Gbps
Capacidade de processamento do UTM	515 Mbps	800 Mbps
Interfaces 10/100/1000	8	8
Interfaces de E/S	1 SRL/2 USB	1 SRL/2 USB
Conexões simultâneas (bidirecionais)	1.700.000	3.300.000
Novas conexões por segundo	20.000	48.000
VLANs	100	200
Licenças WSM (ind.)	4	4
Limite de usuários autenticados	500	500
TÚNEIS VPN		
VPN das filiais de escritórios	50	75
VPN Móvel IPSec	75	100
VPN Móvel SSL/L2TP	75	100

RECURSOS DE SEGURANÇA	
Firewall	Inspeção de pacotes stateful, inspeção profunda de pacotes, firewall de proxy
Proxies de aplicativos	HTTP, HTTPS, SMTP, FTP, DNS, TCP, POP3
roteção contra ameaças	Ataques DoS, pacotes fragmentados e mal formados, ameaças combinadas e muito mais
VoIP	H.323, SIP, configuração de chamada e segurança de sessão
Opções de filtragem	Pesquisa segura em navegador, YouTube para escolas, Google for Business
Assinaturas de segurança	Application Control, IPS, WebBlocker, GAV, Data Loss Prevention, spamBlocker, Reputation Enabled Defense, APT Blocker, Network Discovery e Mobile Security , Threat Detection and Response
VPN E AUTENTICAÇÃO	
Criptografia	DES, 3DES, AES 128-, 192-, 256-bit
IPSec	SHA-2, chave pré-compartilhada IKE e certificados de terceiros
Single sign-on	Compatível com Windows, Mac OS X e sistemas operacionais de dispositivos móveis, RADIUS
Autenticação	RADIUS, LDAP, Windows Active Directory, VASCO, RSA SecurID, banco de dados interno, Duo, SMS Passcode
GERENCIAMENTO	
Registro e notificações	WatchGuard, Syslog, SNMP v2/v3
Interfaces de usuário	Console centralizado (WSM), IU web, CLI com script
Geração de relatórios	O WatchGuard Dimension inclui 100 relatórios predefinidos, resumo executivo e ferramentas de visibilidade
CERTIFICAÇÕES	
Segurança	ICSA Firewall, ICSA IPSec VPN Pendente: CC EAL4+ FIPS 140-2
gurança	NRTL/C, CB
Rede	IPv6 Ready Gold (roteamento)
Controle de substâncias perigosas	WEEE, RoHS, REACH
REDE	
Roteamento	Estático, dinâmico (BGP4, OSPF e RIP v1/v2), VPN baseada em políticas
Alta disponibilidade	Ativo/passivo e ativo/ativo com balanceamento de carga
QoS	8 filas de prioridade, DiffServ e enfileiramento estrito modificado
Atribuição de endereços IP	Estático, DHCP (servidor, cliente e relay), PPPoE e DynDNS
NAT	Estático, dinâmico, 1:1, passagem de IPSec, baseado em políticas, IP virtual para balanceamento de carga de servidores
Agregação de links	802.3ad dinâmico, estático e ativo/reserva
Outros recursos	Independência de portas, balanceamento de carga e failover Multi-WAN, balanceamento de carga de servidores, modo transparente/drop-in

As taxas de transferência são determinadas usando vários fluxos através de diversas portas e podem variar de acordo com o ambiente e a configuração. Entre em contato com o revendedor WatchGuard ou ligue diretamente para a WatchGuard (1-800-734-9905) para obter ajuda e determinar o modelo certo para a sua rede.



ESPECIFICAÇÕES FÍSICAS E DE ENERGIA

Dimensões do produto	431 x 44 x 307 mm (17 x 1,75 x 12,08 pol.)
Dimensões da embalagem	45,7 x 53,3 x 13,3 cm (18 x 21 x 5,25 pol.)
Peso da remessa	7,7 kg (17 lb)
Alimentação CA	100 a 240 VAC detecção automática
Consumo de energia	Vendas 75 Watts (máx), 256 BTU/h (máx)
Montagem em rack	1 kit de montagem em rack 1U incluído

AMBIENTE	OPERACIONAL	ARMAZENAMENTO
Temperatura	0 °C a 40 °C 32 °F a 104 °F	-40 °C a 70 °C -40 °F a 158 °F
Umidade relativa	10% a 85% sem condensação	10% a 95% sem condensação
Altitude	3.000 m a 35° C (0 a 9.843 pés a 95° F)	4.570 m a 35° C (0 a 15.000 pés a 95° F)
MTBF	51.644 horas a 25 °C (77 °F)	

SEGURANÇA FORTE EM CADA CAMADA

Com arquitetura exclusiva para serem os produtos de segurança de rede mais inteligentes, rápidos e efetivos do setor, as soluções da WatchGuard oferecem defesas aprofundadas contra malware, ransomware, botnets, cavalos de troia, vírus, downloads forçados, perda de dados, phishing avançados e muito mais.

ORIENTAÇÃO E SUPORTE ESPECIALIZADOS

Uma assinatura inicial do Suporte acompanha cada dispositivo Firebox M200 e M300. O Suporte Padrão, incluído no Basic Security Suite, oferece garantia de hardware com substituição avançada de hardware, suporte técnico 24 horas por dia, 7 dias por semana, e atualizações de software. Uma atualização para o suporte de nível Gold, incluído no Total Security Suite da WatchGuard, oferece todos os benefícios do suporte padrão, mas escalona os tempos de resposta.

Para obter detalhes, fale com o revendedor autorizado da WatchGuard ou acesse www.watchguard.com.

DIVERSAS OPÇÕES DE COMPRA

A flexibilidade da plataforma integrada da WatchGuard facilita a escolha dos componentes de segurança ideais para a rede da sua empresa. Não importa de você escolhe começar com elementos básicos de segurança ou implementar um arsenal abrangente de defesas de rede, agrupamos serviços de segurança para atender a seus requisitos.

SoluNet
SOLUÇÕES EM REDES
E SUPRIMENTOS LTDA-ME

À
Prefeitura da Estância Turística de São Roque
Divisão de Compras e Licitação
Att: Jessica Zacante
(11) 4784-9682
jznascimento@saoroque.sp.gov.br

REF.: PRESTAÇÃO DE SERVIÇOS DE INFORMÁTICA

APRESENTAÇÃO

Sentimo-nos honrados com a oportunidade de apresentar nossa proposta para prestação de serviços a esta empresa.

A Solunet conta com profissionais especializados atuando nas áreas de ***Software, Hardware e Rede de Comunicação.***

Nossa filosofia é fundamentada em trabalhar em conjunto, buscando prestar um serviço com qualidade, rapidez e baixos custos com objetivo final a solução em informática.

Orçamento nº 952.2017

Proposta 1 – Cluster

Qtde	Produto	Valor unit. R$	Valor Total R$
02	SF SW/Virtual Appliance - UP TO 6 CORES & 8GB RAM	18.750,00	37.500,00
02	SF SW/Virtual Full Guard with Enhanced Support - UP TO 6 CORES & 8GB RAM – licença por 12 meses	33.735,00	67.470,00
	Total.....:		104.970,00

Serviços

Qtde	Produto	Valor unit. R$	Valor Total R$
01	Implantação	6.000,00	6.000,00
01	Treinamento	4.000,00	4.000,00
01	Suporte, manutenção e consultoria em segurança de Redes por 12 meses	12.000,00	12.000,00
	Total.....:		22.000,00

Total do orçamento ..... : 126.970,00

Proposta 2 – Fail Over

Qtde	Produto	Valor unit. R$	Valor Total R$
01	SF SW/Virtual Appliance - UP TO 8 CORES & 16GB RAM	29.221,07	29.221,07
01	SF SW/Virtual Full Guard with Enhanced Support - UP TO 8 CORES & 16GB RAM – licença por 12 meses	52.597,93	52.597,93
	Total.....:		81.819,00

Serviços

Qtde	Produto	Valor unit. R$	Valor Total R$
01	Implantação	6.000,00	6.000,00
01	Treinamento	4.000,00	4.000,00
01	Suporte, manutenção e consultoria em segurança de Redes por 12 meses	12.000,00	12.000,00
	Total.....:		22.000,00

Total do orçamento ..... : 103.819,00

SoluNet
SOLUÇÕES EM REDES
E SUPRIMENTOS LTDA-ME

Fornecedor: Solunet Soluções em Redes e Suprimentos Ltda	
CNPJ: 01.996.783/0001-78	
Endereço/ CEP: R Elisa Rodrigues 36 – Planalto Paulista – SP – 04058-000	
Fone / Fax: 11 23728921	**E-mail: vendas@solunet.com.br**
Nota Fiscal Eletrônica: Sim (x) Não ( )	***Nota Fiscal de: Consumo/ Venda (x) Serviço (x)***

Prazo da Proposta: 90 dias	***Condição (Dias) de Pagamento: 30 dias***	
Entrega: ***Sim (x) Não ( )***	***Condição de Entrega: 45 dias***	
Faturamento Mínimo: valor do produto	***Frete: Sim ( ) Não (x)***	***Valor: R$ 0,00***

Protocolo ICMS 42/09, atualizado pelo protocolo ICMS 85/10:

Cláusula segunda *Ficam obrigados a emitir Nota Fiscal Eletrônica – NF-e, modelo 55, em substituição à Nota Fiscal, modelo 1 ou 1-A, a partir de 1º de dezembro de 2010, os contribuintes que, independentemente da atividade econômica exercida, realizem operações:*
I - destinados à Administração Pública direta ou indireta, inclusive empresa pública e sociedade de economia mista, de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios; (...).

Atenciosamente,

Norival Pessin Junior
Solunet Soluções em Redes e Suprimentos Ltda

Prefeitura da Estância Turística de São Roque
Estado de São Paulo

COTAÇÕES DE PREÇOS

DATA: 20-03-2018

PROCESSO Nº: 240

DESCRIÇÃO	QUANTIDADE	EMB	U/E
CONTRATAÇÃO DE SOLUÇÃO DE FIREWWALL E PROXY COMPLETA COM IMPLANTAÇÃO, TREINAMENTO, SUPORTE, MANUTENÇÃO E CONSULTORIA EM SEGURANÇA DE REDES	9,00		

FORNECEDOR	VALOR UNIT.	VALOR TOTAL
1 .º - 103207 - NETDEEP TECNOLOGIA LTDA - ME	R$ 508,33	R$ 4.575,00
2 .º - 103491 - ALLCOMNET TECNOLOGIA E SISTEMAS - EIRELI - EPP	R$ 1.916,67	R$ 17.250,00
3 .º - 103490 - SOLUNET SOLUCOES EM REDES E SUPRIMENTOS LTDA - ME	R$ 8.651,58	R$ 77.864,25
MÉDIA:	R$ 3.692,19	R$ 33.229,75

Somatória dos Menores Valores: R$ 4.575,00

PREFEITURA DA ESTÂNCIA TURÍSTICA DE SÃO ROQUE

Rua São Paulo, 966 - Bairro Taboão - CEP.: 18.135-125 - São Roque/SP
Fone: (11) 4784-8530 / 4784-8531 - Fax: (11) 4712-4024 - CPNJ: 70.946.009/0001-75

SOLICITAÇÃO DE EMPENHO

DATA: 20-03-2018

SOLICITAÇÃO DE EMPENHO: 625 **PROCESSO:** 240 2018

FORNECEDOR: 103207 - NETDEEP TECNOLOGIA LTDA - ME - CGC/CPF: 11.282.095/0001-08
RUA QUATRO - Nº 958 - ORLANDIA - SP - CEP: 14620000
TEL: 1637263961

MODALIDADE: CD-COMPRA DIRETA- **Tipo Pedido:** Global

CONTRATO: /-1 **ATA:** **Solicitação:** 1306

RECURSO ORÇAMENTÁRIO

DOTAÇÃO: 39 01.01.05.04.122.0008.2008.3.3.90.39.00
ORGÃO: GABINETE DO PREFEITO
UNIDADE: ASSESSORIA DE INFORMÁTICA
JUSTIFICATIVA: LICENÇAS DE USO E SUPORTE TÉCNICO ESPECIALIZADO PARA AS FERRAMENTAS DE FIREWALL E PROXY DE BORDA. CONSIDERANDO AS CRESCENTES AÇÕES DE ATAQUES VIRTUAIS IMPETRADAS POR CRACKERS E O EFETIVO FUNCIONAMENTO DA SOLUÇÃO ORA CONTRATADA, SOMADOS À QUALIDADE DO SUPORTE TÉCNICO PRESTADO, TAL OBJETO TORNOU-SE IMPRESCINDÍVEL NA ESTRUTURA DESTA INSTITUIÇÃO. CONTRAÇÃO ANUAL - PERIODO 9 MESES EM 2018 E 3 MESES PARA 2019

Orçado	Suplementado	Reservado	Empenhado	Liquidado	Pago	Saldo
1.400.000,00	236.800,00	57.579,10	1.559.077,73	364.543,80	9.543,80	20.143,17

QTDE.		U/E	DESCRIÇÃO	MARCA	VLR.UNITÁRIO	VLR.TOTAL
1	9	SE	CONTRATAÇÃO DE SOLUÇÃO DE FIREWWALL E PROXY COMPLETA COM IMPLANTAÇÃO, TREINAMENTO, SUPORTE, MANUTENÇÃO E CONSULTORIA EM SEGURANÇA DE REDES		508,33	4.574,99

Total da Autorização: **4.574,99**

(Quatro Mil Quinhentos e Setenta e Quatro Reais e Noventa e Nove Centavos)

Nome do Comprador
Comprador

Juliana Regina Mesquita Viola
Chefe Serviço Técnico

Débora Freitas Vieira Simões
Chefe de Divisão

Sandra Elisa Scopel Carlini
Diretor(a) da Administração

Cláudio José de Góes
Prefeito Municipal

Enviado 22/03

PREFEITURA ESTÂNCIA TURÍSTICA DE SÃO ROQUE
Rua São Paulo 966 - São Roque - SP B. Taboão
Cep: 18135-125 Telefone: (11) 4784-8500
CNPJ: 70.946.009/0001-75

NOTA DE EMPENHO	Exercício 2018	- Ficha 39
Global	Número : 001688 AF : 625/2018	

DADOS DA DOTAÇÃO ORÇAMENTÁRIA

ORGÃO	: 01	Prefeitura da Estância Turística de São Roque
UNIDADE	: 01	GABINETE DO PREFEITO
SUBUNIDADE	: 05	ASSESSORIA DE INFORMÁTICA
FUNÇÃO	: 04	ADMINISTRAÇÃO
SUBFUNÇÃO	: 122	ADMINISTRAÇÃO GERAL
PROGRAMA	: 0008	MANUTENÇÃO E MODERNIZAÇÃO DO SISTEMA DE INFORMÁTICA
PROJETO/ATIVIDADE	: 2008	INFORMÁTICA
DESPESA	: 3.3.90.39.00	OUTROS SERVIÇOS DE TERCEIROS - PESSOA JURÍDICA
SUBELEMENTO	: 05	SERVIÇOS TÉCNICOS PROFISSIONAIS
FONTE DE RECURSO	: 01 - Tesouro	
COD. APLICAÇÃO	: 110.0000 - GERAL	

DADOS DO CREDOR

FAVORECIDO :103207 NETDEEP TECNOLOGIA LTDA - ME TELEFONE : 1637263961
ENDEREÇO : RUA QUATRO,958 CIDADE ORLANDIA ESTADO : SP
Identidade: CGC/CPF: 11.282.095/0001-08

DADOS DO EMPENHO

Histórico:

LICENÇAS DE USO E SUPORTE TÉCNICO ESPECIALIZADO PARA AS FERRAMENTAS DE FIREWALL E PROXY DE BORDA. CONSIDERANDO AS CRESCENTES AÇÕES DE ATAQUES VIRTUAIS IMPETRADAS POR CRACKERS E O EFETIVO FUNCIONAMENTO DA SOLUÇÃO ORA CONTRATADA, SOMADOS À QUALIDADE DO SUPORTE TÉCNICO PRESTADO, TAL OBJETO TORNOU-SE IMPRESCINDÍVEL NA ESTRUTURA DESTA INSTITUIÇÃO. CONTRAÇÃO ANUAL - PERIODO 9 MESES EM 2018 E 3 MESES PARA 2019

Valor: **(Quatro Mil Quinhentos e Setenta e Quatro Reais e Noventa e Nove Centavos) ,**

Despesa Bruta	**4.574,99**	**Data Empenho**	**23 / 03 / 2018**
Descontos	**0,00**		
Despesa Líquida	**4.574,99**	**Despesa Empenhada**	**4.574,99**

SILVIA CRISTINA SILVA
CHEFE DE SERV. TECNICO DE EMPENHO

CARLA ROGÉRIA AGOSTINHO
DIRETORA DO DEPTO DE FINANÇAS

PREFEITURA DA ESTÂNCIA TURÍSTICA DE SÃO ROQUE

RUA SÃO PAULO, Nº 966 - BAIRRO TABOÃO - CEP.: 18.135-125 - SÃO ROQUE/SP

FONE: (11) 4784-8530 / (11) 4784-8531 - Fax: (11) 4712-4024 - CNPJ 70.946.009/0001-75

AUTORIZAÇÃO DE FORNECIMENTO/SERVIÇO

NÚMERO DA AF: 625 **TIPO:** Global **DATA:** 23-03-2018 **EMPENHO:** 1688/2018

DOTAÇÃO: 39 01.01.05.04.122.0008.2008.3.3.90.39.00 **VLR.DOTAÇÃO:** 4.574,99 **RESERVA:** 406
DIVISÃO: ASSESSORIA DE INFORMÁTICA **VENCIMENTO:**
E. DESPESA: OUTROS SERVIÇOS DE TERCEIROS - PESSOA JURÍDI(**FORMA PGTO.:** PARCELADA MENSALMENTE
LICITACAO: / **MODALIDADE:** CD-COMPRA DIRETA-

FORNECEDOR: 103207 - NETDEEP TECNOLOGIA LTDA - ME
CNPJ/CPF: 11.282.095/0001-08 **INSCRIÇÃO ESTADUAL:**
ENDEREÇO: RUA QUATRO , 958 - CENTRO **EMAIL:**
CIDADE: ORLANDIA / SP **CEP:** 14620000 **TELEFONE:** 1637263961

Destino da Compra: LICENÇAS DE USO E SUPORTE TÉCNICO ESPECIALIZADO PARA AS FERRAMENTAS DE FIREWALL E PROXY DE BORDA. CONSIDERANDO AS CRESCENTES AÇÕES DE ATAQUES VIRTUAIS IMPETRADAS POR CRACKERS E O EFETIVO FUNCIONAMENTO DA SOLUÇÃO ORA CONTRATADA, SOMADOS À QUALIDADE DO SUPORTE TÉCNICO PRESTADO, TAL OBJETO TORNOU-SE IMPRESCINDÍVEL NA ESTRUTURA DESTA INSTITUIÇÃO. CONTRAÇÃO ANUAL - PERIODO 9 MESES EM 2018 E 3 MESES PARA 2019

Local Entrega: 662 - ALMOXARIFADO CENTRAL - RUA: SÃO PAULO, 966 - Bairro TABOÃO - Cep: 18.135-125 SÃO ROQUE - SP

ÍTEM	QTDE.	U/E	DESCRIÇÃO	MARCA	VLR.UNITÁRIO	VLR.TOTAL
1	9,00	SE	.. CONTRATAÇÃO DE SOLUÇÃO DE FIREWWALL E PROXY COMPLETA COM IMPLANTAÇÃO, TREINAMENTO, SUPORTE, MANUTENÇÃO E CONSULTORIA EM SEGURANÇA DE REDES		508,33	4.574,99

Solicitação: 1306 - MAXWEL DA SILVA LIMA
Requisição:
Pr.Compra: 240

Valor Total Pedido: 4.574,99

(Quatro Mil Quinhentos e Setenta e Quatro Reais e Noventa e Nove Centavos)

Observações:
1) Os materiais que não estiverem de acordo com esta autorização de fornecimento serão devolvidos.
2) Colocar o número de processo, numero da AF e o número do empenho na nota fiscal.
3) Horário de recebimento: Almoxarifado Prefeitura das 8:30hs às 16:30hs.
Almoxarifado Farmácia das 7:00hs às 16:00hs.
4) Na emissão da Nota Fiscal a Empresa deverá encaminhar o arquivo XML e DANFE em formato pdf para o e-mail: nfe@saoroque.sp.gov.br
5) O material deverá ser entregue juntamente com a Nota Fiscal Eletrônica.