Folha nº 105
Proc 45/2017

Convite nº 36/2017
Processo nº 45/2017
Objeto: Contratação de empresa especializada na prestação de serviços de implantação de sistema de segurança da informação, composta por hardware e software em toda a rede de dados da Câmara Municipal de Taboão da Serra.

A Câmara Municipal de Taboão da Serra faz saber que encontra-se aberto o **CONVITE Nº 36/2017**, para contratação de empresa especializada na prestação de serviços de implantação de sistema de segurança da informação, composta por hardware e software em toda a rede de dados da Câmara Municipal de Taboão da Serra.

Cópia completa deste Convite e Anexos poderão ser retirados no Setor de Licitações da Câmara Municipal de Taboão da Serra, sito à Estrada São Francisco, 2013, Térreo, Jardim Wanda, Taboão da Serra, São Paulo, de segunda a sexta-feira, no horário das 8h00min às 12h00min e das 14h00min às 16h30min, onde poderão ser obtidas maiores informações.

INFORMAÇÕES PRELIMINARES

A presente licitação será presidida pela Comissão Permanente Julgadora de Licitações, criada pelo Ato da Mesa nº 42/2017 composta pelo Presidente da Comissão: Reinaldo da Silva Borges e os membros, Dr. Isaias Raimundo dos Santos e Flávio Alexandre de Oliveira.

Os licitantes deverão apresentar envelopes fechados, opacos, contendo, no primeiro envelope os **DOCUMENTOS PARA HABILITAÇÃO** e no segundo, a **PROPOSTA DE PREÇOS**, os quais deverão ser entregues, na forma do item 05 e 06 deste edital, até às 14h30min do dia 11 de outubro de 2017, à Comissão, na Diretoria de Licitações da Câmara Municipal de Taboão da Serra, sito à Estrada São Francisco, 2013, Jardim Wanda, Taboão da Serra, São Paulo, onde se realizarão todas as reuniões previstas.

A Comissão reunir-se-á às 14h30min do dia 11 de outubro de 2017, para o recebimento e abertura dos envelopes contendo os **DOCUMENTOS PARA HABILITAÇÃO,** os quais serão conferidos e examinados e rubricados pela Comissão e pelos licitantes presentes que poderão fazer impugnações ou delas se defender. Os licitantes poderão enviar, em seu lugar, representantes legais os quais deverão estar expressamente autorizados, mediante carta em papel timbrado assinado pelos sócios ou diretores da empresa licitante, que estarão autorizados a acompanhar as fases desta licitação.

Havendo expressa renúncia por parte dos representantes das empresas licitantes, ao direito de interposição de recursos referentes às decisões proferidas pela Comissão quanto a **HABILITAÇÃO**, a abertura dos envelopes contendo as **PROPOSTAS** das empresas julgadas habilitadas realizar-se-á no mesmo dia. Caso

em qualquer órgão ou entidade da Administração Pública, que manifestarem interesse com antecedência de até 24(vinte e quatro) horas do prazo previsto para a entrega das propostas.
4.2 Será vedada a participação de empresas:
4.2.1 Declaradas inidôneas por ato do poder público;
4.2.2 Sob processo de concordata ou falência;
4.2.3 Enquadradas nas disposições do artigo 9º da Lei Federal nº 8666/93, atualizada pela Lei Federal 8883/94.
4.3 Somente serão aceitas as propostas devidamente preenchidas e legíveis.
4.4 Nos preços cotados, já deverão estar inclusas todas as despesas e impostos, não cabendo, portanto, a esta administração, nenhum outro ônus a não ser o

também, declaração, conforme modelo constante do **Anexo IV** de que está enquadrada como microempresa ou empresa de pequeno porte.
4.6 A não apresentação da documentação devidamente regularizada, conforme previsto no inciso 1º do Art. 43 da Lei supracitada, no prazo concedido, acarretará na inabilitação da empresa.
4.7 Fica a critério dos licitantes a participação na abertura dos envelopes, no dia e horário estabelecido neste Convite, desde que devidamente identificados.
4.8 Se o licitante participante infringir quaisquer das cláusulas constantes deste Convite e/ou Anexos, a Comissão de Julgamento de Licitações, declará-lo **DESCLASSIFICADO**.

5. DA HABILITAÇÃO (ENVELOPE Nº01)
5.1 O envelope contendo a **HABILITAÇÃO** deverá ser fechado, indevassável, opaco contendo externamente nome do proponente, número do convite e;
5.1.1 Registro comercial, no caso de empresa individual;
5.1.2 Ato constitutivo, estatuto ou contrato social em vigor e alterações subsequentes, devidamente registrado, em se tratando de sociedades comerciais, e, no caso de sociedades por ações, acompanhados da Ata Arquivada da Assembleia da ultima eleição de seus Administradores;
5.1.3 Prova de Inscrição no Cadastro Nacional de Pessoas Jurídicas - CNPJ;
5.1.4 Certidão Negativa de Débitos - CND perante o INSS;
5.1.5 Certificado de Regularidade de situação perante o FGTS – CRF;
5.1.6 Certidão Negativa de Débitos Trabalhistas – (CNDT);
5.1.7 Declaração de que esta enquadrada como Microempresa ou Empresa de Pequeno Porte nos termos do art. 03º da Lei Complementar nº 123/2006.
5.2 Declaração de Qualificação Técnica;
5.3 Atestado de Visita Técnica;
5.4 Os documentos solicitados poderão ser apresentados por fotocópias autenticadas na forma da Lei ou acompanhados dos originais para autenticação pela Comissão Julgadora de Licitações na reunião de abertura dos envelopes de **"HABILITAÇÃO"** ou por publicação em órgão na Imprensa.

6. DA PROPOSTA (ENVELOPE Nº02)
6.1 O envelope contendo a **PROPOSTA DE PREÇO** deverá ser fechado, indevassável, opaco contendo externamente nome do proponente e número do convite.
6.2 A proposta deverá ser formulada, conforme **Anexo II**, via original, em idioma nacional, digitada, sem emendas ou rasuras, assinada em seu final pelo representante legal da proponente e rubricada nas demais folhas.
6.3 O preço ofertado com a porcentagem do BDI;
6.4 O licitante deverá cotar o valor total;
6.5 A omissão ou exclusão, no custo de quaisquer itens específicos, não exime o licitante de executá-los dentro do preço proposto;
6.6 Os preços devem ser expressos em algarismos, em reais, apurados na data da apresentação da proposta, sem inclusão de qualquer encargo financeiro ou previsão inflacionária.

6.7 Validade da proposta: o prazo de validade das propostas não poderá ser inferior a 30 (trinta) dias, contados a partir da data de abertura das propostas.

7. FORMA DE APRESENTAÇÃO DOS ENVELOPES

7.1 O proponente deverá apresentar 02 (dois) envelopes fechado e opaco, contendo as seguintes indicações no envelope:

À CÂMARA MUNICIPAL DE TABOÃO DA SERRA
CONVITE Nº 36/2017
RAZÃO SOCIAL DA PROPONENTE E RESPECTIVO CNPJ
ENVELOPE 1 – DOCUMENTOS DE HABILITAÇÃO

À CÂMARA MUNICIPAL DE TABOÃO DA SERRA
CONVITE Nº 36/2017
RAZÃO SOCIAL DA PROPONENTE E RESPECTIVO CNPJ
ENVELOPE 2 – PROPOSTA DE PREÇO

08. DA ABERTURA DOS ENVELOPES E JULGAMENTO

8.1 O presente Convite será processado e julgado de acordo com o procedimento estabelecido no artigo 43 da Lei 8666/93, atualizada pela lei federal 8883/94.

8.2 No dia, local e hora designados, na presença dos licitantes ou de seus representantes legais que comparecerem ao ato, a Comissão iniciará os trabalhos, examinando o envelope proposta, o qual será rubricado pelos seus membros e representantes presentes, procedendo-se a seguir à sua abertura.

8.3 Depois de abertos os envelopes, as propostas serão tidas como imutáveis e acabadas, não sendo admitidas quaisquer providências posteriores tendentes a sanarem falhas ou omissões.

8.4 As propostas serão examinadas e rubricadas pelos membros e representantes dos licitantes presentes.

8.5 As propostas que apresentarem erros manifestos de cálculos será corrigido automaticamente pela Comissão.

8.6 Desta fase será lavrada Ata circunstanciada, que será assinada pelos membros da Comissão e representantes presentes, constando da mesma toda e qualquer declaração.

8.7 Ocorrendo à desclassificação de todas as propostas, a Administração poderá fixar aos licitantes o prazo de 05 (cinco) dias úteis para a apresentação de nova documentação ou de outras propostas escoimadas das causas referidas neste item.

8.8 Se ocorrer à suspensão da reunião para julgamento e a mesma não puder ser realizada no mesmo dia, o resultado será afixado no quadro de avisos da Câmara Municipal de Taboão da Serra, para conhecimento dos interessados.

09. CRITÉRIO DE JULGAMENTO DAS PROPOSTAS

9.1 A classificação das propostas será efetuada em função do preço total por item. Sendo considerada vencedora a proposta que apresentar o menor preço por hora.

9.2 Não será considerada qualquer oferta de vantagem não prevista neste Convite, nem preço ou vantagem baseada na proposta de outros concorrentes.

9.3 Serão desconsideradas as propostas que não atenderem as exigências deste Convite.

9.4 Serão desclassificadas as propostas apresentadas em desacordo com este Convite, com borrões, rasuras, entrelinhas, emendas, ressalvas, sem assinatura ou omissões. Fica a juízo da CPL a classificação por irregularidade formal que não afete o conteúdo ou idoneidade da proposta.

9.5 Em caso de empate (absoluta igualdade) entre as propostas, obedecido ao disposto no parágrafo 2º, do artigo 3º, da Lei 8666/93, a classificação se dará por sorteio, em ato público, para o qual todos os licitantes serão convocados.

9.6 A adjudicação e a homologação serão afixadas nos quadros de aviso da Câmara Municipal de Taboão da Serra.

9.7 Ao órgão licitante fica facultado o direito de, com devida fundamentação, aceitar a proposta que lhe parecer mais vantajosa, rejeitar todas, anular ou revogar a licitação nos termos da Lei Federal 8666/93, atualizada pela Lei Federal 8883/94.

10. DAS CONDIÇÕES DE PAGAMENTO

10.1 O pagamento será efetuado no prazo de até 05 (cinco) dias, após a implantação do sistema, devidamente comprovados pelo responsável direto em sua Divisão de Tesouraria, situada à Estrada São Francisco, 2013, Jd. Wanda, Taboão da Serra/SP, CEP 06765-001, mediante a apresentação da Nota Fiscal dos Serviços.

11. FORMA DE APRESENTAÇÃO DAS NOTAS FISCAIS

11.1 O proponente vencedor deverá apresentar as Notas Fiscais/ Fatura desta licitação no Setor de Tesouraria da Câmara Municipal de Taboão da Serra, contendo a seguinte informação: Convite n. ° 27/2017, com a descrição do objeto.

12. DA CONTRATAÇÃO

12.1. Quando a convocada a subscrever o contrato, a adjudicatária deverá fazê-lo no prazo máximo de 05 (cinco) dias úteis, da data do recebimento da convocação, atendendo as seguintes disposições:

12.2. O prazo para assinatura do contrato será de 15 (quinze) dias úteis da data da homologação, podendo ser prorrogado por igual período, quando solicitado por escrito, durante seu transcurso, e ocorrendo motivo justificado e aceito pela Administração.

12.3. Havendo desistência ou recusa da adjudicatária em assinar o contrato no prazo estabelecido, é facultado a Administração convocar os licitantes

remanescentes, respeitada a ordem de classificação, para fazê-lo em igual prazo e condições, sem prejuízo das penalidades previstas em Lei.
12.4. São de inteira responsabilidade do licitante vencedor do certame todas as obrigações pelos encargos previdenciários, fiscais, trabalhistas e comerciais resultantes da execução do contrato.
12.5. A licitante vencedora se responsabilizará, ainda, por todas as despesas oriundas do contrato, assim como por eventuais danos ou prejuízos causados a terceiros ou à Câmara Municipal de Taboão da Serra, resultantes de sua culpa ou dolo ou de seus respectivos prepostos na execução do contrato.
12.6. Ao licitante classificado em primeiro lugar será adjudicado o objeto do certame, sendo que após a regular homologação pela Autoridade Superior e providências administrativas, será ele convocado a assinar o contrato administrativo no prazo máximo de 05 (cinco) dias.

13. PENALIDADES
13.1 Pela inexecução total ou parcial do ajuste, objeto da presente licitação, a Administração poderá, garantida a prévia defesa, aplicar ao adjudicatário as seguintes sanções:
13.1.2 advertência;
13.1.3 multa nos termos previstos na Lei Federal 8666/93, atualizada pela Lei Federal 8883/94;
13.1.4 multa de 10% (dez por cento) por inexecução parcial do contrato, o qual incidirá sobre o valor total do contrato, devidamente reajustado na data do efetivo pagamento da multa;
13.1.5 multa de 30% (trinta por cento) por inexecução total do contrato, ou recusa em assinar o mesmo, a qual incidirá sobre o valor total do contrato, devidamente reajustado na data do efetivo pagamento da multa;
13.1.6 suspensão temporária de participar de licitação e impedimento de contratar com a Administração por prazo superior a 02 (dois) anos;
13.1.7 declaração de inidoneidade para licitar ou contratar com a Administração, enquanto perdurarem os motivos da punição ou até que seja promovida a reabilitação, perante a autoridade que aplicou a penalidade;
13.2 A aplicação das multas é independente da aplicação das demais sanções.

14. DOS RECURSOS
14.1 Somente serão aceitos os recursos previstos na Lei 8666/93, atualizada pela Lei Federal 8883/94, os quais deverão ser protocolados na Câmara de Taboão da Serra.
14.2 Decairá do direito de impugnação dos termos do Convite aquele que, tendo-o aceito sem objeção, venha a apontar, depois do julgamento, falhas ou irregularidades que o viciariam, hipótese em que tal comunicação não terá efeito de recurso.

15. DAS INFORMAÇÕES COMPLEMENTARES

15.1. Fica facultada à Comissão Julgadora ou autoridade superior, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou a complementar a instrução do processo;
15.2. Todos os prazos previstos serão contados excluindo-se o dia do início e incluindo-se o dia do vencimento. Se qualquer dos prazos aqui previstos recaírem em dia em que não haja expediente nesta Câmara Municipal, o mesmo transferir-se-á para o primeiro dia útil subseqüente;

16. DAS DISPOSIÇÕES GERAIS
16.1 As partes elegem a Comarca de Taboão da Serra, para qualquer procedimento relacionado ao processamento desta licitação e ao cumprimento do contrato dela originado.
16.2 Fica facultada a Comissão Julgadora ou autoridade superior, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou a complementar a instrução do processo.
16.3 A Câmara Municipal poderá, a qualquer tempo, por despacho motivado, anular, adiar ou revogar a presente licitação, no todo ou em parte, sem que por este motivo, tenham os licitantes direitos a qualquer indenização ou compensação.

17. DO HORÁRIO E LOCAL PARA OBTENÇÃO DE ESCLARECIMENTOS
17.1 Este convite será afixado para conhecimento e consulta dos interessados no quadro de avisos da Câmara Municipal de Taboão da Serra, situada a Estrada São Francisco, 2013, Térreo, Jardim Wanda, Taboão da Serra – São Paulo.
17.2 Maiores esclarecimentos poderão ser obtidos no Setor de Licitações, localizado à Estrada São Francisco, 2013, Térreo, Jardim Wanda, Taboão da Serra – São Paulo, no horário das 8h00min às 14h00min, até o último dia previsto para entrega dos envelopes.

18. ANEXOS INTEGRANTES DO EDITAL
18.1. Anexo I – Memorial Descritivo;
18.2. Anexo II – Modelo de Proposta de Preços;
18.3. Anexo III – Minuta Contratual;
18.4. Anexo IV – Declaração de M.E ou E.P.P ;
18.5. Anexo V – Orçamento Estimativo
18.6. Anexo VI – Declaração de Qualificação Técnica
18.7. Anexo VII – Atestado de Visita Técnica

Taboão da Serra, 03 de outubro de 2017.

Joice Marques da Silva
PRESIDENTE DA CÂMARA MUNICIPAL DE TABOÃO DA SERRA

CÂMARA MUNICIPAL TABOÃO DA SERRA SP

- Anexo I - Memorial Descritivo –

1 – DETALHAMENTO

A- INTRODUÇÃO

Este memorial foi elaborado com a finalidade de descrever e orientar a Implantação do Serviço de Solução Integrada de Firewall, composta por Hardware e Software de segurança de toda rede de dados da Câmara Municipal de Taboão da Serra.

B- DISPOSIÇÃO

Todo e qualquer serviço será executado por profissionais habilitados, e a contratada assumirá integral responsabilidade pela boa execução e eficiência dos serviços, bem como por eventuais danos decorrentes da realização do referido trabalho.

C- DESCRIÇÃO DOS SERVIÇOS

A empresa contratada deverá implantar sistema de segurança da informação com solução integrada de Firewall NEXT GENERATION, composta de Hardware e Software de segurança da informação do tipo UTM (Unified Threat Management), entendendo-se como tais o conjunto de serviços e recursos de: Filtro de pacotes com controle de estado, Filtro de conteúdo web, Interceptação SSL, Filtro de aplicações, Controle da web 2.0, Inspeção com proteção contra ataques de Malwares, vírus, worm, e aplicativos maliciosos, integrar soluções do tipo (IDS/IPS, ATP, QoS, Balanceamento de serviços, Redundância de links, VPN, DHCP e DNS). Com a capacidade de integrar todos os recursos em um único dispositivo.

Todos os produtos e serviços deverão ser orçados para um período mínimo de contrato de 12 meses.

D- TAREFAS A SEREM EXECUTADAS

a) Implantação de servidor Appliance de UTM de 1000 Mbps de capacidade de firewall com garantia e atualização para 12 meses;
b) A solução de firewall deverá ser integrada com tecnologia de proteção de rede stateful packet inspection, serviços e recursos modulares de Filtro de conteúdo web, Interceptação SSL, Controle da web 2.0, Inspeção com proteção contra ataques de malwares, vírus, worms e aplicativos maliciosos (IDS/IPS), QoS, VPN e Filtro de aplicações;
c) APL UTM BB; Software License e UTM Subscription Advance;
d) Instalação e treinamento técnico dos servidores/usuários.

2. ESPECIFICAÇÕES TÉCNICAS

Para a prestação do serviço a contratada deverá providenciar e dispor:

2.1. Appliance de UTM de 1000 Mbps de capacidade de firewall com garantia e atualização para 12 meses;

2.2. O equipamento deve se instalar em mesa com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 1U (44,45mm) da referida mesa;

2.3. Dispor de fonte de alimentação com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;

2.4. Deverão ser fornecidos todos os cabos de energia, serial (RS-232/RJ45), para instalação e funcionamento do dispositivo;

2.5. Possuir led indicador on/off, disco e devices de rede;

2.6. Possuir throughput mínimo de 1000 Mbps para tráfego TCP;

2.7. Possuir throughput mínimo de 2000 Mbps para tráfego UDP;

2.8. Possuir throughput mínimo de 200.000 (duzentas mil) conexões simultâneas;

2.9. Suportar no mínimo 16.000 (Dezesseis mil) novas conexões por segundo;

2.10. Possuir throughput mínimo de 400 Mbps para tráfego HTTP/ HTTPS via Proxy;

2.11. Possuir throughput mínimo de 100 Mbps para tráfego HTTP/ HTTPS com inspeção SSL via Proxy;

2.12. Possuir throughput mínimo de 90 Mbps para tráfego HTTP/ HTTPS com inspeção SSL + Inspeção ATP via Proxy;

2.13. Possuir throughput mínimo de 180 Mbps para tráfego IPS;

2.14. Possuir throughput mínimo de 150 Mbps para tráfego ATP;

2.15. Possuir throughput mínimo de 285 Mbps para tráfego VPN IPSEC com criptografia (AES-128);

2.16. Possuir throughput mínimo de 200 Mbps para tráfego VPN SSL com criptografia (AES-128);

2.17. Suportar no mínimo 30 conexões de usuários concorrentes para VPN SSL;

2.18. Possuir no mínimo 4 (quatro) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade;

2.19. Possuir no mínimo 2(duas) devices de rede GbE By-pass;

2.20. Possuir mínimo de 4 GB de memória RAM;

2.21. Possuir dispositivo de armazenamento interno de no mínimo 120 GB padrão SSD;

2.22. Possuir no mínimo 1 (uma) porta console de conexão padrão RJ45 para acesso a interface de comando CLI especifica para esta finalidade, utilizando cabo do tipo serial RS-232/RJ-45;

2.23. Possuir pelo menos 2 (duas) portas USB para conexão de dispositivos externos;

3. ESPECIFICAÇÕES GERAIS DE SOFTWARE

3.1. A Solução deve ser uma solução UTM "Unified Threat Management" Gerenciador Unificado de ameaças, integrada com os demais recursos e serviços, deve ser capaz de instalar todos os recursos e serviços em um mesmo hardware.

4. RECURSOS E SERVIÇOS GERAIS

4.1. Deve suportar tecnologia de Firewall Stateful Packet Inspection;

4.2. Possuir conexão entre a estação de gerência e Appliance no modo criptografado tanto em interface gráfica, quanto em CLI (linha de comando). O Acesso a interface de administração deve ser via WEB sob o protocolo HTTPS com ergonomia voltada a usabilidade;

4.3. Gerenciamento do tráfego e estatísticas sumarizadas através de um painel de controle;

4.4. Possuir sistemas de alertas e notificações do sistema em tempo real na interface WEB e envios automáticos por e-mail;

4.5. Interface responsiva compatível com dispositivos móveis;

4.6. Interface em português e inglês;

4.7. O sistema deve permitir o acesso à interface de gerenciamento WEB por qualquer interface de rede configurada;

4.8. Permitir a criação de perfis de administração baseado em ACL (Acess List), de forma a possibilitar a definição de diversos administradores para o dispositivo, cada um responsável por determinada tarefa da administração;

4.9. Permitir a conexão simultânea de vários administradores, com poderes de alteração de configurações e/ou apenas de visualização das mesmas;

4.10. Permitir criar as definições de ACL (Acess List) completa por administrador, sendo possível especificar os direitos, como: somente Visualizar ou Editar "Alterar, Excluir, Cadastrar";

4.11. Permitir auditoria do sistema com log das ações dos administradores por tipo de recurso e período;

4.12. Possuir porta console para possíveis manutenções no produto;

4.13. Acesso via WEB a console shell para gerenciamento através de interface de linha de comando CLI (Command Line Interface). Configurações básicas via interface CLI como suporte a comandos para debug deverão ser suportadas por esta interface;

4.14. A interface CLI deve suportar a configuração de roteamento dinâmico no mínimo para os protocolos BGP, OSPF, RIP1 e RIP2 com suporte a interface Vty;

4.15. Possuir um Certificado digital (CA – Certificado de Autoridade) padrão X.509, nativo com chaves de 2048 bits, para os processos de autenticação do usuário, utilização do proxy SSL e em todas as conexões de serviços com o Appliance.

4.16. A solução deve manter um canal de comunicação segura, com criptografia baseada em certificados entre todos os componentes que fazem parte da solução de firewall, gerência, armazenamento de logs e emissão de relatórios;

4.17. Permitir a integração com qualquer autoridade certificadora válida emissora de certificados X509 que deve seguir os padrões descritos na RFC 2459.

4.18. Capacidade para criação de objetos com a finalidade de facilitar a administração e configuração do sistema, deve atender no mínimo os seguintes tipos de objetos: endereço IP, endereço MAC, Portas de serviços e protocolos, atendendo no mínimo os seguintes protocolos (TCP, UDP, ICMP, IGMP, AH, EGP, ESP, GRE, RSVP, e SCTP), tabela de horário, período com especificação de data/hora inicial e final, tabela de palavras chaves com a possibilidade de especificar expressões regulares, tipos de conteúdo de arquivos (content types);

4.19. Possuir um sistema de armazenamento remoto com suporte a conexões do tipo SMB, NFS e Disco (USB-HDD);

4.20. Possuir mecanismo que permita a realização de cópias de segurança (backups) do sistema e restauração remota, através da interface gráfica, a solução deve permitir o agendamento diário ou semanal;

4.21. As cópias de segurança (backups) devem ser armazenadas em dispositivos remotos do tipo NFS (Network File System) ou Disco externo (USB-HDD);

4.22. O sistema deve permitir configurar o período ou número de cópias que deseja manter no repositório remoto e executar a manutenção de período automaticamente.

4.23. As cópias de segurança devem ser salvas compactadas e criptografadas de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup;

4.24. O sistema ainda deve contemplar um recurso de cópia de segurança do tipo snapshot, que contemple a cópia completa das configurações dos serviços e recursos do sistema;

4.25. Deve possibilitar a restauração do snapshot através da interface web de qualquer ponto remoto, de modo a contribuir para uma restauração imediata sem a necessidade de reinicialização do sistema;

4.26. Suporte e integração com servidores de Network Time Protocol (NTP) para atualização de data e hora do sistema, o que padroniza e evita problemas com o horário de verão;

4.27. Atualização automática do sistema para correções e releases. O sistema de atualização deve permitir agendamento para verificação diária da base de atualizações do fabricante.

4.28. As atualizações devem ser disponibilizadas no intervalo máximo de 15 dias. Não podendo ultrapassar este período;

4.29. Permitir desabilitar update automático;

4.30. Efetuar controle de tráfego e monitor por estado de conexão no mínimo para os seguintes protocolos (TCP, UDP, ICMP, IGMP, AH, EGP, ESP, GRE, RSVP e SCTP) baseados nos endereços de origem, destino e porta;

4.31. Suportar o Internet Protocol Versões 4 (IPv4);

4.32. Suporte à Interfaces Ethernet;

4.33. Suportar o protocolo 802.1q, para uso e segmentação da rede com VLANs;

4.34. Suportar o protocolo 802.1x, para autenticação RADIUS;

4.35. Suporte a interfaces do tipo MACVLAN;

4.36. Suportar o protocolo 802,1ax e 802.3ad (LACP), Link Aggregation Control Protocol;

4.37. Suporte à interfaces DSL;

4.38. Suporte à roteamento estático;

4.39. Suporte ao protocolo SNMP;

4.40. A solução deve suportar no mínimo o funcionamento com 2 (dois) equipamentos idênticos, de forma que funcione com tolerância a falhas (ativo/passivo);

5. AUTENTICAÇÃO

5.1. Suporte à múltiplos domínios de autenticação, mínimo 3(três) domínios;

5.2. Permitir o cadastro dos usuários e grupos em base de dados própria por meio da interface de administração WEB do dispositivo;

5.3. Suporte à sincronismo de usuários e grupos com servidores Windows AD® e Servidores LDAP;

5.4. Permitir a utilização de LDAP, LDAP/SSL para a autenticação de usuários;

5.5. Permitir a utilização de autenticação RADIUS para sincronismo de contas e sessões;

5.6. Permitir o login de usuários de forma transparente ao efetuar logon na rede para plataformas Windows 2008 e 2012 Servers (sem a necessidade de o usuário digitar novamente a senha), para todos os serviços suportados, considerando assim a autenticação do usuário, como uma autenticação unificada entre a plataforma Windows e o Appliance Firewall NG UTM;

5.7. Permitir o controle de acesso por usuário, para todas as plataformas com browser através de autenticação via portal WEB para todos os serviços suportados, de forma que um determinado usuário tenha seu perfil de acesso automaticamente carregado;

5.8. Possuir suporte a um sistema de autenticação do tipo Captive Portal capaz de redirecionar de forma automática a autenticação, deve ser compatível com autenticação Windows AD®, LDAP, RADIUS e LOCAL;

5.9. O Captive Portal deve suportar o protocolo HTTPS para a tela de autenticação do usuário e para administração dos serviços de Captive Portal para o usuário;

5.10. A solução deve permitir em seu portal de autenticação o cadastro de novos usuários, permitindo controle por área, para usuários convidados o Captive Portal solicitará informações para cadastro no sistema, enquadrando automaticamente à um perfil de acesso previamente configurado;

5.11. O sistema de Captive Portal deve ser capaz de aplicar uma política geral e gerenciar a sessão do usuário autenticado:

5.12. Controlar o número de sessões concorrentes por usuário;

5.13. Controlar o número de tentativas de autenticação não autorizada;

5.14. Bloquear o endereço IP de origem das tentativas de autenticação não autorizada;

5.15. Definir o tempo de bloqueio do endereço IP das tentativas de autenticação não autorizada;

5.16. Definir tempo de sessão por inatividade;

5.17. Identificar endereço IP;

5.18. Identificar endereço MAC;

5.19. Permitir o administrador efetuar logout de sessão de qualquer usuário através da interface de gerenciamento WEB da solução de firewall;

5.20. Os usuários devem ter acesso à alguns recursos tais como: alterar dados pessoais; alterar senha para os casos de usuário do tipo local; fazer o download do Certificado de Autoridade (CA) e acesso ao Termos de Uso;

6. SEGURANÇA

6.1. Prover a condição de configuração de uma Política padrão por agrupamento de devices ou zonas de rede, determinando origem e destino por tipo de agrupamento;

6.2. Possibilitar exigir autenticação para a política padrão;

6.3. Capacidade para trabalhar com conversão de endereços e portas (NAT/NAPT) conforme RFC 3022; ser capaz de aplicar mascaramento de pacotes do tipo: SNAT (source nat) por endereço IP de origem; SNAT (masquerade) por device de origem; DNAT (dnat) mascaramento de destino por endereço IP/porta de destino e Nat-T em VPN IPSec;

6.4. Prover mecanismos de segurança configuráveis, que permita habilitar proteção contra ataques do tipo: "Denied of Service; Portscan; Pacotes inválidos; SYN Flood; ICMP Flood";

6.5. Possuir mecanismo que permita habilitar e desabilitar recursos do tipo: "ICMP Echo/Request – ping; ICMP Redirect; ICMP Broadcast; Source Routing; Checksum; Log Inválidos; TCP be liberal";

6.6. Possuir mecanismo de configuração para o controle de tipos de conexão possibilitando definir limites máximos para cada tipo de controle das conexões do protocolo TCP;

6.7. Possuir mecanismo de configuração para o controle de conexão possibilitando definir limites de timeout para as conexões genéricas;

6.8. Possuir mecanismo de configuração para o controle de conexão do protocolo ICMP possibilitando definir limites de timeout;

6.9. Possuir mecanismo de configuração para o controle de conexão do protocolo UDP possibilitando definir limites de timeout;

6.10. Detectar automaticamente e inserir regras de bloqueio temporárias para varreduras de portas efetuadas contra o dispositivo ou contra qualquer máquina protegida por esse, mesmo que realizados em períodos maiores que 1 (um) dia;

6.11. Possuir politicas padrões de entrada para os serviços nativos do firewall, por agrupamento de device ou zonas de rede, podendo exigir ou não autenticação, com possibilidade de aplicar ações de bloqueio, permissão, inspeção IPS ou inspeção ATP;

6.12. Permitir definir as políticas de entrada para os serviços nativos do firewall, podendo aplicar filtros no acesso por: usuário, grupos, endereço IP de origem, endereço IP de destino e horário;

7. PROXY

7.1. Possuir Proxy nativo para tráfego HTTP, HTTPS, versões 1.0 e 1.1, FTP;

7.2. Deve possibilitar a conexão de tráfego para outros serviços e que contemplem a conexão em proxys HTTP, tais como: XMPP, SIP, H323, SMTP, POP3, IMAP, RTSP, TELNET e outros;

7.3. Deve permitir a configuração para outras portas de serviços;

7.4. Deve permitir implementar proxy transparente para os protocolos HTTP e HTTPS, de forma a dispensar a configuração dos browsers dos dispositivos clientes para a utilização das características o serviço;

7.5. Deve permitir implementar proxy configurado para os protocolos HTTP, HTTPS, FTP e SOCKS;

7.6. Deve permitir o armazenamento em cache de conteúdo trafegado pelo protocolo HTTP e HTTPS;

7.7. Possuir sistema de cache interno, armazenando requisições WEB em disco local e memória;

7.8. Deve permitir a definição do tamanho mínimo dos objetos salvos em cache no disco;

7.9. Deve permitir a definição do tamanho máximo dos objetos salvos em cache em memória;

7.10. Deve atender a estrutura de navegação através de hierarquia de proxy com e sem autenticação;

7.11. Deve permitir operar sem interceptação SSL.

7.12. Possibilitar a integração com servidores de cache WEB externos;

7.13. Deve ser capaz de armazenar cache dinâmicos para as atualizações Microsoft Windows Update®;

7.14. Deve ser capaz de armazenar cache dinâmicos de streaming no mínimo para endereços do Youtube® e MSN Vídeos®;

7.15. Deve ter capacidade de armazenar em cache dinâmicos conteúdo do Facebook®, Google Maps® e Sourceforge Downloads®;

7.16. Deve possuir a capacidade de excluir URL's específicas do cache web, configurável por listas de palavras chaves com suporte inclusive a expressões regulares;

7.17. Deve ter suporte à integração com antivírus HTTP através de hierarquia de proxy;

7.18. Possuir mecanismos de integração à interceptação SSL com suporte a conexões de proxy transparente ou proxy configurado;

7.19. Ter a capacidade de análise de HTTP e HTTPS, pelo Antimalware se determinados tipos de arquivos baseados na extensão contém vírus antes de entregá-lo ao usuário e suportar ao menos 2 scanners;

7.20. Ter a capacidade de trabalhar como Anti-Virus de Gateway permitindo a análise de arquivos específicos por extensão;

7.21. Permitir o gerenciamento de quarentena de Malware;

7.22. Permitir realizar Filtro de Conteúdo por Autoridade Certificadora;

7.23. Permitir desabilitar interceptação de SSL por domínio;

8. SISTEMA DE PROTEÇÃO AVANÇADA CONTRA AMEAÇAS

8.1. Possuir sistema de proteção avançada contra ameaças (ATP) nativo;

8.2. O sistema de ATP deve monitorar e analisar o tráfego da rede, identificar aplicativos e ameaças de ataques direcionados e persistentes e efetuar os respectivos bloqueios.

8.3. Deve ser baseado em uma lista de assinaturas eletrônicas que atue em tempo real analisando a camada de aplicação, capaz de identificar o conteúdo dos pacotes, fazer log (registros) das assinaturas trafegadas, inspecionar os pacotes e efetuar o descarte automático do pacote quando identificado assinaturas de pacotes maliciosos, inapropriados para o uso no ambiente corporativo;

8.4. A base de assinaturas do sistema de ATP nativo deverá ser fornecida pelo período do contrato;

8.5. A base de assinaturas deve possuir mínimo de 2(duas) modalidades de assinaturas, atendendo a identificação de ameaças e aplicativos;

8.6. Possuir um mínimo de 31 mil (trinta e um mil) assinaturas;

8.7. O fabricante deve garantir o fornecimento de atualizações regulares dentro do período de assinatura contratado;

8.8. Deve permitir a atualização automática das assinaturas por meio de agendamento diário;

8.9. Possuir capacidade de inspecionar e bloquear em tempo real, ameaças do tipo: activex, malware, malware-backdoors, ataques P2P, trojans, worms, user_agents, pua (adware, p2p, toolbars) malwares para mobile, blacklist, botcc, exploits-kits, file-executable, file-flash, file-identify, file-image, file-java, file-multimedia, file-office, file-other, file-pdf, games, inappropriate e vulnerabilidades conhecidas;

8.10. Possuir uma ferramenta de bloqueio de execução de aplicativos, integrado a base de Antivírus e Antimalware;

8.11. Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos do tipo: ads, cloud, colaboração, download, e-mail, games, mobile, p2p, proxy, remote, redes sociais; storage, streaming, update, voip e web.

8.12. Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de VoIP tais como: Hotline, Asterisk, Linphone, SIP, Skype, Xlite SIP, X-Pro SIP, Cisco SIP, OpenSIP, Bria, ClearSea e Nero SIP;

8.13. Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de Redes Sociais tais como: Aol Instant Messenger, Badoo, BaiduHi, Airtime, Blogger, BoldChat, ChatON, China.com, Facebook, Flickr, FC2, Fring, Google Analytics, Google App, ICQ, Linkdin, Meetup, MSM Messenger, Netlog, Skype, Tinder, Tuenti, Twitter, WhatssApp, WeChat e Zoho Chat;

8.14. Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos e transferências de arquivos do tipo P2P (peer to peer) tais como: BitTorrent, Gnutella, FastTrack, IceShare, Napster, Shareman e de Storages, tais como: Dropbox, Easy-share, Google Drive, Megashare, MegaUpload, Rapidshare, OneDrive, Yahoo Box, SoundCloud e Filemail, DivShare;

8.15. Possuir mecanismo de bloqueio para listas de reputação de endereço IP catalogadas no mínimo para 6(seis) categorias, capaz de permitir seleção

por categorização, elas devem atender as seguintes classificações: spam, reputation, malware, attacks, anonymous e abuse;

8.16. Possuir mecanismo de bloqueio e proteção por localização GeoIP para uma lista mínima de 250 Países e Repúblicas;

8.17. Deve possuir mecanismos de integração nas conexões via proxy, a partir da interceptação SSL. Possuir capacidade de inspeção profunda de pacotes (Deep Package Inspection - DPI), conseguir inspecionar aplicações criptografadas incluindo todo o payload;

8.18. Suportar exceção de ameaças por assinatura; IP de origem ou IP de destino;

8.19. Suportar exceção de aplicativos por assinatura; IP de origem ou IP de destino;

8.20. Suportar exceção para base de reputação IP por endereço IP;

8.21. Suportar exceção para a base de localização GeoIp por endereço IP;

8.22. Ação de Bloqueio do pacote ou reset da conexão em tempo real;

8.23. Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre as "ameaças detectadas" e as "ameaças bloqueadas";

8.24. Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre os "aplicativos detectados" e os "aplicativos bloqueados";

8.25. Deve possuir mecanismos para gerar log dos registros das incidências, classificados em pelo menos 3 (três) níveis de impacto: "baixo; médio e alto";

8.26. Gerar registro do tipo Top Level, dos 10(dez) mais, inclusive da relação de eventos entre usuários e ameaças, usuário e aplicativos, aplicativos e ameaças identificados e bloqueados;

8.27. Todos os logs e registros devem permitir ser gerados por período: "diário ou mensal";

8.28. Possuir mecanismos para inspecionar, identificar e detectar os aplicativos e sub aplicativos trafegados via proxy e classificá-los de acordo com a base de assinaturas;

8.29. Possuir mecanismos para inspecionar, identificar e detectar as ameaças e ataques do tráfego geral, incluindo o trafego via proxy e classificá-los de acordo com a base de assinaturas;

8.30. Deve permitir o bloqueio em caso de detecção dos aplicativos e ou ameaças e atacantes, com base nas políticas de cada assinatura;

9. SISTEMA DE PREVENÇÃO CONTRA INTRUSÃO

9.1. Possuir sistema de prevenção contra intrusão de atacantes (IPS) nativo;

9.2. O Sistema de IPS deve monitorar, analisar o trafego e proteger a rede contra ataques internos e externos e utilizar técnicas de varredura e identificação que filtrem e bloqueie os pacotes atacantes e descarte o pacote com conteúdo de código malicioso;

9.3. Deve ser baseado na identificação de assinaturas de tipos de ataques e aplicações com vulnerabilidades conhecidas. O IPS deve contemplar uma base de assinaturas capaz de identificar o método de ataque com base em modelos de comportamento, características dos protocolos de rede, sistemas operacionais, inclusive comandos executados e esse conjunto de informações deve permitir que o pacote malicioso seja identificado e bloqueado em tempo real pelo IPS.

9.4. Possuir pelo menos 18000 mil (dezoito mil) assinaturas;

9.5. O fabricante deve garantir o fornecimento de atualizações regulares dentro do período de assinatura contratado;

9.6. Deve permitir a atualização automática das assinaturas por meio de agendamento diário;

9.7. A base de assinaturas deve contemplar um mínimo de 65 (sessenta e cinco) categorias, atendendo a identificação de ameaças e atacantes;

9.8. A solução deve ser capaz de detectar e prevenir as seguintes ameaças: Exploits e vulnerabilidades específicas de clientes e servidores, mau uso de protocolos, comunicação outbound de malware, tentativas de tunneling, e ataques genéricos;

9.9. A solução deve prover mecanismos de proteção contra ataques dos serviços de rede e aplicações, protegendo pelo menos os seguintes serviços: aplicações web, serviços de, DNS, FTP, SNMP, Telnet, TFTP, serviços Windows (Microsoft Networking) e VoIP.

9.10. A solução deve prover mecanismos de proteção contra ataques as assinaturas relacionadas a web-server, IIS, Apache, MSSql, MySql para que seja usado para proteção específica de Servidores Web;

9.11. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS), Exploits, Attack Response;

9.12. Detecção de ataques de RPC (Remote Procedure Call);

9.13. Deve prover mecanismos de Proteção contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol);

9.14. Deve prover mecanismos de Proteção contra ataques de ICMP (Internet Control Message Protocol);

9.15. Deve possuir mecanismos de integração nas conexões via proxy, a partir da interceptação SSL. Possuir capacidade de inspeção profunda de pacotes (Deep Package Inspection - DPI), conseguir inspecionar pacotes criptografados incluindo todo o payload;

9.16. Suportar exceção de ameaças por assinatura; IP de origem ou IP de destino;

9.17. Ação de Bloqueio do pacote ou reset da conexão em tempo real;

9.18. Deve possuir mecanismo para gerar log dos registros das incidências, classificados em pelo menos 3 (três) níveis de impacto: "baixo; médio e alto";

9.19. Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre os "ataques detectados" e os "ataques bloqueados";

9.20. Gerar registro do tipo Top Level, dos 10(dez) mais, inclusive da relação de eventos entre os tipos de ataques e usuários, os graus de impacto e usuários, ataques identificados e bloqueados;

9.21. Todos os logs e registros devem permitir ser gerados por período: "diário ou mensal";

9.22. Possuir mecanismos para inspecionar, identificar e detectar as ameaças e ataques do tráfego geral, incluindo o trafego via proxy, e classificá-lo de acordo a base de assinaturas;

9.23. Deve permitir o bloqueio em caso de detecção de ameaças e atacantes, com base nas políticas de cada assinatura;

10. QOS

10.1. Deve permitir especializar as redes de forma a melhorar sensivelmente a qualidade de conexão, tratando de forma diferenciada e especifica as transmissões que exijam maior e melhor qualidade da rede;

10.2. Deve possuir mecanismo que permita criar controles por fila de prioridade, mínima de 5(cinco) níveis;

10.3. Deve ser capaz de alterar a velocidade dos acessos por nível de prioridade;

10.4. Deve ser capaz de criar limites de banda máxima por fila de prioridade;

10.5. Deve ser capaz de criar garantia de banda mínima por fila de prioridade;

10.6. Deve permitir a habilitação do controle de velocidade permitindo especificar a largura de banda ou velocidade Downstream e Upstream de cada barramento ou device;

10.7. Priorização de pacotes com suporte às tecnologias de tratamento ToS (Type of Service) e DSCP (DiffServ Code Point);

10.8. Permitir modificação de valores ToS para a priorização de roteamento dos pacotes;

10.9. Implementar no mínimo 5(cinco) níveis de roteamento e tipos de serviços, com configuração e marcação para códigos ToS através da interface gráfica;

10.10. Permitir modificação de valores DSCP dos pacotes para o DiffServ;

10.11. Implementar no mínimo 20 (vinte) classes de serviço distintas, com configuração do mapeamento e marcação para códigos DSCP através da interface gráfica;

11. BALANCEAMENTO DE LINK

11.1. Deve ser capaz de segmentar e priorizar o tráfego através das interfaces de rede;

11.2. Deve contemplar a função de roteamento por prioridade de links;

11.3. Deve ser "tolerante à falhas", ou seja, possuir recurso de FailOver;

11.4. Deve possuir mecanismos de controle de falhas de link, capaz de aplicar testes da disponibilidade em tempo real. Estes testes devem retornar para o sistema o status atual de cada link e em caso de falhas do link principal, este recurso deverá alterar o "gateway padrão" do sistema para o próximo link da lista de prioridades de links;

11.5. O serviço de FailOver de links deve possibilitar que os testes e monitoramento sejam realizados através do protocolo ICMP para endereços de hosts externos;

11.6. O monitoramento no protocolo ICMP deve permitir inserir múltiplos endereços para verificação e o link principal somente será marcado como inativo se todos os hosts externos pararem de responder;

11.7. Deve possuir as seguintes opções de configurações para o monitoramento do link que fazem parte do FailOver e Balanceamento de link:

11.8. Intervalo de monitoramento;

11.9. Quantidade tentativas de testes por host ou número de falhas necessárias antes de marcar o link como inativo;

11.10. Permitir utilizar um link como principal e outro como secundário. O tráfego apenas será redirecionado (FailOver) quando o principal ficar indisponível, retornado ao estado anterior quando o principal ficar ativo novamente;

11.11. Deve suportar regras de roteamento dos serviços de saída do próprio dispositivo de firewall, podendo selecionar entre os links, inclusive definindo prioridade do tráfego;

11.12. Suportar o uso simultâneo de múltiplos links em um mesmo firewall, de provedores distintos ou não.

11.13. Permitir o balanceamento de links, inclusive com IPs dinâmicos para ADSL ou outra tecnologia de banda larga que não utilize IP Fixo;

11.14. Deve contemplar o recurso de balanceamento de links por políticas de segurança; podendo ser aplicadas por: origem, destino, conteúdo web, horário ou período de data e hora inicial e final, controles de tipo de conteúdo, tipo de pacote; políticas de mascaramento; políticas de proxy; usuário e grupos;

12. CONTROLE DE APLICATIVOS WEB

12.1. O controle de aplicativos web deve possuir mecanismos de detecção capaz de tomar medidas contra o tráfego de rede indesejado por tipo de aplicativo e sub aplicativos em uso, deve ser baseado em decodificadores de assinaturas e protocolos.

12.2. O controle desses aplicativos devem permitir inspecionar, permitir ou bloquear estes acessos nas conexões HTTP e HTTPS através de proxy transparente ou proxy configurado, inclusive a definição de quais usuários, grupos de usuários, redes, devices ou agrupamentos de devices podem utilizar ou não estes recursos, definindo inclusive dentro das suas características quais recursos de cada aplicativo poderão ser utilizados.

12.3. A base deve contemplar um número mínimo de 790 aplicativos e sub aplicativos diferentes, catalogados e classificados em categorias, mínima de 24 categorias;

12.4. Possuir mecanismos de criação de regras que possibilite definir políticas de segurança de maneira simplificada, sem a necessidade de especificar endereço de origem ou destino das aplicações, para as tomadas de ação;

12.5. Reconhecer no mínimo aplicações do tipo redes sociais, aplicativos peer to peer, acesso remoto, games, streamings, aplicativos de lojas on line, mensageiros instantâneos, colaboração, vídeo conferência, e-mails, fóruns, bloggers, storage, proxy anônimos, antivírus entre outras;

12.6. Deve contemplar assinaturas que identifique pelo menos os aplicativos e sub aplicativos tais como: Youtube®, Facebook®, Twitter®, Linkedin®, Tumblr®, Bittorrent®, Gnutella®, AIM®, Baidu®, Syflex®, Logmein®, Join.me®, DropBox®, Onedrive®, Apple iCloud®, Amazon®, Ebay®, ITunnes®, Blospot®, Instagram®, Flickr®, Photoshop®, Picasso®, Myspace®, Netflix®, Justin TV®, Megavideo®, Skype®, Viber®, Whatsapp®, Yahoo Messenger®, Spotify®, Wunderlist®, Webex®, Gismodo®, Google News®, Google Docs®, Google Earth®, Google Translator®, Google Finance®, Money Control®, Morningstar®, Playstation®, Wii®, Xbox Live®;

12.7. Ser capaz de identificar assinaturas de aplicações de uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações de proxys que utilizam táticas evasivas via comunicações criptografadas, tais como Ultrasurf, Vtunnel, Zenguard, Privax, Proxydotorg;

12.8. O recurso deve de forma objetiva controlar aplicativos web 2.0 com a finalidade de melhorar o desempenho da rede e evitar improdutividade do grupo de usuários da rede;

13. FILTRO DE CONTEÚDO WEB

13.1. O filtro de conteúdo web deve possuir mecanismos de detecção capaz de tomar medidas contra o tráfego de rede indesejado dependendo da URL ou categoria web, deve ser baseado em uma lista de URL's classificadas por tipo de conteúdo;

13.2. O filtro de conteúdo web deve permitir inspecionar, permitir ou bloquear estes acessos nas conexões HTTP e HTTPS através de proxy transparente ou proxy configurado, inclusive a definição de quais usuários, grupos de usuários, redes, devices ou agrupamento de devices, podem acessar ou não as diversas categorias identificadas;

13.3. O filtro de conteúdo web deve possuir base de dados catalogada com mínimo de 40 milhões de URL's e classificada em no mínimo 80 categorias;

13.4. A solução deve possuir mecanismos de criação de regras que possibilite definir políticas de segurança de maneira simplificada, sem a

necessidade de correlacionar endereços de origem e destino das URL's ou categorias web para as tomadas de ação;

13.5. A solução de filtro de conteúdo deve suportar a ação de forçar a pesquisa segura independente da configuração do navegador (browser) da estação de trabalho do usuário. Esta funcionalidade não permitirá que os sites de busca retornem resultados considerados inapropriados. Esta funcionalidade deve ser suportada no mínimo para os buscadores "Google®", "Bing®" e "Yahoo®";

13.6. Deve possuir mecanismos de filtragem de métodos HTTP a fim de otimizar e melhorar a eficiência do tráfego web, deve comtemplar filtros do tipo: put, get, checkout, connect, delete, head, link, post, search e trace;

13.7. Deve permitir criar base de categorias personalizadas a partir de listas de URL's com suporte a lista de palavras chaves e expressões regulares;

13.8. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;

13.9. Permitir a criação de filtros para arquivos e dados pré-definidos;

13.10. Os arquivos devem ser identificados por extensão e assinaturas;

13.11. Suporte a identificação de arquivos compactados, executáveis, imagens e multimídias, a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

13.12. Deve oferecer a opção de bloquear controles ActiveX e Java Scripts que possam comprometer o acesso web dos usuários;

13.13. Deve oferecer a opção de cota de tempo em horas ou minutos de navegação web por dia;

13.14. Deve oferecer a opção de cota de tráfego em MB de navegação web por dia;

13.15. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, Compactados, Executáveis, ISOs e etc) identificados sobre aplicações (HTTP, HTTPS e FTP) inclusive oferecendo a opção de controle de tamanho máximo de download por navegação;

13.16. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, Compactados, Executáveis, ISOs, etc) identificados sobre aplicações (HTTP, HTTPS e FTP) inclusive oferecendo a opção de controle de tamanho máximo de upload por navegação;

13.17. Deve suportar mecanismos de filtro e controle de login no Google® por domínio, permitindo ao administrador especificar os domínios permitidos;

13.18. O sistema de filtro de conteúdo poderá ser aplicado por definição de horário ou período de validade do filtro; podendo ou não especificar usuários, grupos de usuários, rede ou agrupamento de device para todos os recursos de filtragem e controles estabelecidos;

14. POLÍTICAS DE SEGURANÇA DO FIREWALL

14.1. O sistema deve integrar os respectivos recursos e serviços de integração com o firewall: NAT, proxy; filtro de conteúdo web, filtro de aplicações web, QoS, FailOver e balanceamento de links, de acordo as especificações técnicas descritas a fim de propiciar um sistema capaz de tratar o tráfego da rede em camadas, garantindo a segurança dos dados;

14.2. Estes recursos integrados devem permitir o tratamento do tráfego em camadas, de modo granular com o suporte a interceptar o tráfego SSL, identificar malwares e ações mal-intencionadas que utilizam o protocolo HTTPS para burlar firewalls, o sistema deve interceptar estas conexões, analisar e enviar os pacotes para tomadas de ações;

14.3. Deve também permitir a inspeção destes pacotes, detectar e prevenir dos ataques de intrusos, operando em conjunto com o firewall, impedir que acessos externos e/ou remotos executem rotinas de invasão. Executando ação pró ativa de bloqueio dos ataques;

14.4. Deve permitir gerar políticas de segurança capaz de filtrar os pacotes, integrar aos recursos de tratamento de filtro de conteúdo, filtro de aplicações, gerenciamento e controle dos pacotes definindo controle de banda por níveis de velocidade e garantia de banda por prioridade.

14.5. Deve permitir o roteamento estático por device, por endereço IP, serviços, usuários, grupos de usuários, para cada link de internet podendo distribuir o balanceamento de carga entre múltiplos links de internet ou ainda definir um roteamento exclusivo sem a opção de redundância ou FailOver;

14.6. As políticas de segurança devem permitir integrar em uma mesma interface interativa a definição de uma única política que atenda todos os recursos integrados com o firewall;

14.7. As políticas de segurança devem tomar ações do tipo: permitir, bloquear e inspecionar para o tráfego IPS ou Inspecionar para o tráfego ATP;

14.8. As políticas de segurança devem atender as especificações por prioridade, se o conteúdo do tráfego se enquadrar as definições da política, a mesma deve ser aplicada ignorando as políticas de menor prioridade;

14.9. Deve permitir o agrupamento de políticas respeitando as regras de negócio;

14.10. Deve permitir reordenação sempre que necessário;

14.11. Deve suportar mecanismos de balanceamento de links por política, inclusive com devices do tipo VLAN ou MACVLAN (endereços virtuais);

14.12. Deve ser permitido desabilitar uma política de segurança sem que seja necessário remove-la da lista;

14.13. A interação da interface ainda deve prover um recurso ou mecanismo para expandir a política, ou seja, permitir a visualização com as informações de filtros e a ação que compõe a regra;

15. VPN IPSEC

15.1. A solução deve prover comunicação através de túneis VPN "Virtual Private Network" ou "Rede virtual Privada". Ter como principal finalidade utilizar os recursos da rede pública "Internet" para conectar redes remotas.

15.2. Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereços inválidos possam se comunicar através da Internet;

15.3. Deve suportar VPN IPSEC Túnel site to site ou site to client;

15.4. Deve suportar VPN IPSEC RAS - Acesso remoto IPSEC;

15.5. Deve suportar os protocolos padrões de VPN: IPSEC, ESP, IKE e IKE versão 2;

15.6. A solução de VPN deve operar o padrão IPSEC, de acordo com as RFCs 2401 a 2412, de modo a estabelecer canais de criptografia com outros produtos que também suportem tal padrão;

15.7. O suporte aos protocolos e algoritmos de autenticação e integridade IKEv1 e IKEv2 de acordo a RFC 7296, de modo a estabelecer canais de autenticação e criptografia com outros produtos que suportem tal padrão;

15.8. Deve possuir suporte a algoritmos de criptografia IKE: 3DES, AES, Blowfish;

15.9. Deve possuir suporte a algoritmos de integridade IKE: md5, sha1, sha256, sha384 e sha512;

15.10. Deve possuir suporte a algoritmos de criptografia ESP: DES, AES, Blowfish e Camélia;

15.11. Deve possuir suporte a algoritmos de integridade ESP: md5, sha1, sha256, sha384, sha512, aesxcbc e aescmac;

15.12. Suporte ao menos à 5 Diffie-Hellman distintos;

15.13. A solução deve atender a suporte IKEv2 com suporte a fragmentação, de acordo a RFC 7383;

15.14. Deve possuir funcionalidade que permita estabelecer túneis de VPN com Appliances da mesma solução ou outras soluções de VPN implementadas atrás de firewalls, através de encapsulamento UDP, de acordo a RFC 3947;

15.15. Implementar os esquemas de troca de chaves manual, para os protocolos IKE e IKEv2 através de chave compartilhada (Pré-Shared Key);

15.16. Suportar Main Mode e Aggressive mode em IKE v1;

15.17. Possuir funcionalidade Dead Peer Detection (DPD) ou similar;

15.18. Suportar VPN Redundante (Failover) reestabelecimento automático da VPN IPSEC sobre um segundo enlace caso haja falha no enlace principal);

15.19. Suporte a conexão por FQDN "Full Quality Domain Name";

15.20. Deve permitir habilitar, desabilitar os túneis de VPN IPSEC

15.21. A solução deve prover recursos de controle de conexão no tratamento do protocolo IKE que possibilite definir parâmetros dos tempos de vida das conexões e retransmissão e da autenticação IKE;

15.22. O sistema de VPN IPSEC RAS deve funcionar como um provedor de VPN para clientes, de modo a atribuir aos clientes endereços IPs não válidos, colocando-os, virtualmente, em uma rede local estendida;

15.23. No modo VPN IPSEC RAS deve ser possível configurar o endereço/range IP a ser atribuída a interface de rede virtual do cliente de VPN, bem como sua máscara de rede, endereços dos servidores DNS, endereço dos servidores WINS, rota default e rotas para sub-redes;

15.24. O modo VPN IPSEC RAS deve suportar autenticação integrada X-Auth (Integração Windows AD, PAM LDAP e base de autenticação local) para usuários do firewall;

15.25. Deve possuir mecanismos de autenticação com suporte a EAP (MSCHAP2) para clientes VPN IPSEC Windows;

15.26. Compatibilidade com clientes VPN nativos para os sistemas operacionais iOS 7 ou superior, Android 4.4.4 ou superior, MacOS X 10.6 ou superior, Linux 2.6.36 ou superior, Windows 7 ou superior;

16. VPN SSL

16.1. A solução deve prover comunicação através de VPN SSL que permita um usuário remoto devidamente autorizado a utilizar um navegador WEB moderno para acessar com segurança diversos serviços da rede privada;

16.2. A solução deve suportar acesso com chaves de criptografia com tamanho igual ou superior a 128 bits, de forma a possibilitar a criação de canais seguros ou VPNs através da Internet;

16.3. A VPN SSL deve possibilitar o acesso a toda infraestrutura de acordo com a política de segurança, através de um plug-in ActiveX e/ou Java;

16.4. O acesso deve oferecer versatilidade, facilidade de uso, e controles específicos de grupos e usuários em cada modalidade de aplicação e deve estar disponível através de um portal WEB.

16.5. Deve prover acesso via túnel SSL utilizando um navegador sem a necessidade de um cliente instalado na estação remota, e ser compatível com o navegador Mozilla Firefox versão 47;

16.6. Deve ser compatível com as plataformas operacionais: MS-Windows, Linux, MacOS;

16.7. Deve possuir mecanismos de tunelamento de aplicações através de um portal web, com suporte a desvio de porta (Port Forward) para as aplicações internas;

16.8. Permitir acesso interno e externo ao portal web;

16.9. Deve suportar as seguintes modalidades de aplicações: Aplicações Túnel do tipo cliente-servidor, Aplicações de acesso remoto tais como: VNC, SSH, Terminal Service, Aplicações web do tipo HTTP e HTTPS, Compartilhamento de rede do tipo SMB;

16.10. Deve possuir suporte a autenticação integrada X-Auth (Integração Windows AD, PAM LDAP e base de autenticação local) para usuários do firewall;

17. SERVIÇOS DE REDE (DDNS, DNS E DHCP)

17.1. A solução de UTM integrada deve permitir integração à serviços do tipo DDNS (Dynamic DNS);

17.2. Possuir suporte à publicação de hosts dinâmicos para os provedores de serviços: NO-IP e Dyndns;

17.3. Deve contemplar um mecanismo de atualização automática do DDNS por agendamento (update);

17.4. O serviço de DDNS deve ser compatível com Interface DSL ou PPOE;

17.5. O sistema também deve prover um recurso de redirecionamento DNS para provedores de DNS recursivo a fim de disponibilizar acesso a serviços de resolução de nomes remotos; permitir a consulta recursiva a partir dos redirecionamentos de DNS;

17.6. Permitir a configuração de acesso e redirecionamento por device de rede;

17.7. Suporte a cache de DNS;

17.8. Possuir mecanismos de proteção capaz de identificar ataques que disponibilizem servidores DNS válidos com autoridades sobre domínios configurados para responder um TTL (Time to live) muito baixo, inibindo a ação de guardar cache, o sistema deve possibilitar a proteção contra ataques que alteram a resposta a pesquisa de DNS para um endereço IP dinâmico de servidores com códigos maliciosos;

17.9. O sistema de proteção a este tipo de resposta (pesquisa de domínios com TTL muito baixo) deve possuir a opção de exceção para endereços de hosts locais e por domínios possibilitando especificar hosts e domínios confiáveis que não queira guardar cache;

17.10. Deve permitir DNS Redirect por listas de hosts;

17.11. A solução de UTM integrada deve fornecer um serviço de DHCP (Dynamic Host Configuration Protocol) Server e DHCP Relay;

17.12. Deve possuir mecanismo de configuração e distribuição de pool de endereços IPs por device de rede, com suporte a interfaces do tipo ethernet, VLAN, inclusive interface MACVLAN (Virtuais);

17.13. Deve permitir a distribuição do pool de endereços IPs por filtro de grupo ou objeto de endereço MAC; permitir a distribuição de endereço IP fixado ao endereço MAC.

17.14. A distribuição dos dados de configurações de serviços de rede deve contemplar a distribuição de Gateway ou roteamento, a definição de um sufixo de DNS; lista de endereço de servidores de DNS e servidores Wins;

17.15. Deve permitir a definição do tempo de vida do DHCP para a renovação do endereço IP entregue;

18. CLUSTER

18.1. A solução deve suportar funcionamento com 2 (dois) ou mais equipamentos idênticos, de forma que funcione com tolerância a falhas (ativo/passivo);

18.2. Os dois dispositivos devem ser ligados em paralelo, com réplicas das configurações entre eles. O dispositivo secundário não estará tratando o tráfego, ele entrará em funcionamento para tratamento de tráfego somente quando o dispositivo principal ficar inoperante;

18.3. Deverão ser capazes de manter o sincronismo de todos os itens de configuração e serviços, exemplo: Políticas de segurança, Configurações de segurança do firewall, Certificado de autoridade, Contas administrativas, Configuração de VPN, Configurações de rede, Roteamento estático, Roteamento dinâmico, Perfis, bases de antivírus, filtros web, IPS e ATP;

18.4. A alta disponibilidade deve ter persistência de sessão e detecção de falhas por protocolo VRRP;

18.5. O Sincronismo dos servidores deve ser por interface exclusiva;

19. RELATÓRIOS

19.1. A geração de relatórios deve ser centralizada e disponibilizada através da interface WEB da solução e disposta em um painel de controle de gerenciamento.

19.2. A geração dos relatórios detalhados deve ser opcional e configurável por tipo de relatório: proxy, ataques e ameaças, aplicativos e firewall;

19.3. A solução deve disponibilizar a geração de relatórios acessíveis, fáceis de usar e baseados na web que ofereça visão em tempo real, relatórios sumarizados, gráficos e históricos detalhados.

19.4. Os relatórios devem propiciar ao administrador base concreta de análise fornecendo uma visão profunda de como a rede e os computadores estão sendo utilizados, permitindo-se entender e reforçar quando necessário as regras de conformidade.

19.5. A solução também deve através da interface de administração web, permitir administradores visualizar os relatórios dos usuários.

19.6. Acesso centralizado e consistente a todos os logs sumarizados e eventos do sistema com a opção de verificação "Diária" e "Mensal" dos registros e ainda com a opção de extração no formato "PDF" e "CSV".

19.7. Suporte à geração em PDF para os relatórios estatísticos;

19.8. Deve ser capaz de gerar e manter os relatórios detalhados no mínimo por 7(sete) dias;

19.9. Deve suportar exportação dos relatórios detalhados no formato CSV;

19.10. Possuir um mecanismo de arquivamento dos relatórios gerados para download, o arquivamento deve ser mantido pelo período mínimo de 1(hum) mês;

19.11. Possuir um serviço de manutenção de limpeza dos registros de estatísticas e relatórios extraídos nos formatos CSV e PDF, mantendo os registros por um período mínimo de 30(trinta) dias;

19.12. A manutenção dos relatórios detalhados deve ser rotacional, automático e deve manter um período mínimo de 7 dias;

19.13. O sistema deve possuir um mecanismo de log que permita enviar os arquivos de log para outro servidor do tipo SYSLOG, especificando IP e porta;

19.14. Deve ser capaz de gerar relatório Online com (B.I) Business Intelligence para filtro na busca de relatórios;

19.15. Deve contemplar relação de eventos entre os itens de relatórios do proxy;

19.16. Deve contemplar relação de eventos entre os itens de relatórios das ameaças e aplicativos;

19.17. Deve contemplar os eventos de detecção do AntiMalware;

19.18. Deve contemplar relação de eventos entre os itens de relatórios dos atacantes;

19.19. A empresa fabricante da solução deve garantir que todos os relatórios detalhados devem ser assinados através de uma chave de integridade (key) que garanta a confiabilidade dos dados, atendendo ao Marco Civil nº 12.965/2014;

20. REGISTROS E LOGS DO SISTEMA

20.1. Deve atender os registros e logs do sistema das respectivas informações de gerenciamento por dispositivo: relatórios e gráficos gerais do sistema;

20.2. Gerar gráfico estatístico do sistema contendo informações do total de tráfego de rede e histórico diário por hora em (KB/ MB/ GB/ TB);

20.3. Gerar gráfico estatístico do sistema contendo informações do total de tráfego web via proxy e histórico diário por hora em (KB/ MB/ GB/ TB);

20.4. Gerar gráfico estatístico do sistema contendo informações do total de ameaças e aplicativos detectados pelo sistema de proteção de ameaças

persistentes, tipo ATP e contemplar inclusive um histórico diário por hora em (KB/ MB/ GB/ TB);

20.5. Gerar gráfico estatístico do sistema contendo informações do total de ataques detectados pelo sistema de prevenção de intrusos, tipo IPS (Inspection Prevention System) e contemplar inclusive um histórico diário por hora em (KB/ MB/ GB/ TB);

20.6. Gerar gráfico estatístico do sistema contendo informações do total de tráfego de rede e histórico mensal por dia em (KB/ MB/ GB/ TB);

20.7. Gerar gráfico estatístico do sistema contendo informações do total de tráfego web via proxy e histórico mensal por dia em (KB/ MB/ GB/ TB);

20.8. Gerar gráfico estatístico do sistema contendo informações do total de ameaças e aplicativos detectados pelo ATP (Advanced Threats Protection) e histórico mensal por dia em (KB/ MB/ GB/ TB);

20.9. Gerar gráfico estatístico do sistema contendo informações do total de ataques detectados pelo IPS (Inspection Prevention System) e histórico mensal por dia em (KB/ MB/ GB/ TB);

20.10. Gerar histórico dos top 10 (dez) com o total do tráfego de rede em (KB/ MB/ GB/ TB) por: usuários, grupos, serviços/protocolos; regras de conformidade e categorias web;

20.11. Gerar histórico dos top 10 (dez) alertas de segurança dos ataques detectados pelo firewall com o total de hits;

20.12. Gerar histórico dos top 10 (dez) aplicativos web (ATP) com o total de hits;

20.13. Gerar histórico das top 10 (dez) ameaças APT (Advanced Persistent Threats) detectados pelo ATP com o total de hits e classificação do tipo de impacto na rede;

20.14. Gerar histórico dos top 10 (dez) ataques detectados pelo (IPS) com o total de hits e classificação do tipo de impacto na rede;

20.15. Gerar gráfico estatístico do sistema contendo informações de desempenho como: (%) percentual de uso de processamento (CPU), (%) percentual de entrada/saída (I/O), (%) percentual de carga média (LOAD), (%) percentual de utilização de disco e (%) percentual de consumo de memória (RAM);

20.16. Gráfico estatístico do consumo de banda, mínimo de 5 (cinco) níveis de prioridade em (B/ KB/ MB/ GB/ TB/);

20.17. Gráfico estatístico em tempo real do tráfego total da rede (RX/ TX);

20.18. Gráfico estatístico do sistema contendo histórico sobre o tráfego dos devices de rede (RX/ TX) e um serviço de monitoração em tempo real para cada device de rede;

20.19. A solução deve possuir um sistema de monitoração de tráfego para as novas conexões, podendo aplicar filtros por: endereço IP de origem, endereço IP de destino, serviços com a especificação de porta e protocolo. O serviço de monitoração deve retornar os dados especificados nos filtros e a respectiva regra de conformidade;

20.20. A solução deve possuir um sistema de monitoração de tráfego para as conexões estabelecidas, podendo aplicar filtros por: endereço IP de origem, endereço IP de destino, serviços com a especificação de porta e protocolo, inclusive limitando o quadro de respostas até 10 (dez) conexões estabelecidas. O serviço de monitoração deve retornar os dados especificados nos filtros, o total de tráfego em (KB/ MB/ GB/ TB), a velocidade em (bps/ kbps/ Mbps/ Gbps/ Tbps) e o número de pacotes trafegados;

21. RELATÓRIOS E GRÁFICOS GERAIS DO TRÁFEGO WEB VIA PROXY

21.1. Gerar gráficos estatísticos do tráfego WEB via Proxy contendo as seguintes informações: total das requisições, total das requisições bloqueadas;

21.2. Gerar gráfico, histórico ou resumo diário, da relação de eventos entre o total de trafego web via proxy dos acessos permitidos e os acessos bloqueados no intervalo de tempo de 1 (uma) hora;

21.3. Gerar gráfico, histórico ou resumo mensal, da relação de eventos entre o total de tráfego web via proxy dos acessos permitidos e os acessos bloqueados no intervalo de tempo de 1 (uma) hora;

21.4. Gerar gráfico, histórico ou resumo diário, da relação de eventos entre o total de trafego web via proxy dos acessos direto e os acessos ao cache no intervalo de tempo de 1 (uma) hora;

21.5. Gerar gráfico ou resumo mensal do total da relação de eventos entre o tráfego web via proxy dos acessos direto e os acessos ao cache no intervalo de tempo de 1 (hum) dia;

21.6. Gerar histórico dos Top Level 10 (dez) com o total do tráfego em (KB/ MB/ GB/ TB) e o total dos acessos, com a opção de ordenação por tráfego e por acessos, das regras de conformidade permitidas e tipos de conteúdo permitidos;

21.7. Gerar histórico dos Top Level 10 (dez) com o total do tráfego em (KB/ MB/ GB/ TB), tempo em (horas/ minutos) e total de acessos, com a opção

de ordenação por tráfego, por tempo, e por acessos, das categorias permitidas e aplicativos permitidos;

21.8. Gerar histórico dos Top Level 10 (dez) "usuários" com o total do tráfego em (KB/ MB/ GB/ TB), tempo em (horas/ minutos), velocidade em (bps, Kbps/ Mbps/ Gbps/ Tbps), total de acessos permitidos e total de acessos bloqueados, com a opção de ordenação por tráfego, por tempo, permitidos e bloqueados;

21.9. Gerar histórico dos Top Level dos 10 (dez), inclusive a relação de eventos entre "usuários" e as "categorias web" com o total do tráfego em (KB/ MB/ GB/ TB), tempo em (horas/ minutos), Velocidade em (bps, Kbps/ Mbps/ Gbps/ Tbps), total de acessos permitidos e total de acessos bloqueados, com a opção de ordenação por tráfego, por tempo, permitidos e bloqueados;

21.10. Gerar histórico dos Top Level 10 (dez), inclusive a relação de eventos entre os "usuários" e os "aplicativos web" com o total do tráfego em (KB/ MB/ GB/ TB), tempo em (horas/ minutos), Velocidade em (bps, Kbps/ Mbps/ Gbps/ Tbps), total de acessos permitidos e total de acessos bloqueados, com a opção de ordenação por tráfego, por tempo, permitidos e bloqueados;

21.11. Gerar histórico dos Top Level 10 (dez), dos "bloqueados" com o total das tentativas de acesso, das regras de conformidade bloqueadas, categorias bloqueadas, aplicativos web bloqueados e tipos de conteúdo bloqueados;

21.12. A solução deve possuir um sistema de monitoração da navegação WEB via Proxy em tempo real por filtro do tipo: servidor, origem (endereço IP ou usuário), URL de destino e porta de serviço. O serviço de monitoração deve retornar o tempo de tráfego em (hora/ minuto/ segundo), a origem (endereço IP ou usuário), o total de tráfego em (B/ KB/ MB/ GB/ TB), a velocidade em (bps/ Kbps/ Mbps/ Gbps/ Tbps) e a URL de destino;

22. RELATÓRIOS E GRÁFICOS GERAIS DO TRÁFEGO ATP

22.1. Gerar gráficos estatísticos do tráfego ATP contendo as seguintes informações: total de ameaças detectadas, total de ameaças bloqueadas, total de aplicativos detectados, total de aplicativos bloqueados;

22.2. Gerar gráfico, histórico ou resumo diário, da relação de eventos entre o total de trafego ATP das ameaças detectadas a as ameaças bloqueadas no intervalo de tempo de 1 (uma) hora;

22.3. Gerar gráfico, histórico ou resumo diário, da relação de eventos entre o total de trafego ATP dos aplicativos detectados e os aplicativos bloqueados no intervalo de tempo de 1 (uma) hora;

22.4. Gerar gráfico, histórico ou resumo mensal, da relação de eventos entre o total de trafego ATP das ameaças detectadas e as ameaças bloqueadas no intervalo de tempo de 1 (hum) dia;

22.5. Gerar gráfico, histórico ou resumo mensal, da relação de eventos entre o total de trafego ATP dos aplicativos detectados e os aplicativos bloqueados no intervalo de tempo de 1 (hum) dia;

22.6. Gerar gráficos estatísticos do tráfego ATP contendo as informações do total de ameaças e aplicativos detectados por grau de risco e impacto na rede, mínimo de 3 (três) tipos de graus de risco ou impacto;

22.7. Gerar históricos ou resumos diários do total de tráfego ATP das ameaças e aplicativos detectados por grau de risco e impacto na rede, mínimo de 3 (três) tipos de graus de impacto no intervalo de tempo de 1 (uma) hora;

22.8. Gerar históricos ou resumos mensais do total de tráfego ATP das ameaças e aplicativos detectados por grau de risco e impacto na rede, mínimo de 3 (três) tipos de graus de impacto no intervalo de tempo de 1 (hum) dia;

22.9. Gerar histórico do Top Level 10 (dez) "detectados", com o total de detecções e o tipo de impacto das ameaças e aplicativos;

22.10. Gerar histórico dos Top Level 10 (dez), inclusive a relação de eventos entre as "ameaças" e os "usuários" com o tipo de impacto, total de detecções e o total de bloqueados, com a opção de ordenação por detecções e bloqueados;

22.11. Gerar histórico dos Top Level 10 (dez), inclusive a relação de eventos entre os "aplicativos" e os "usuários" com o total de detecções e o total de bloqueados, com a opção de ordenação por detecção e bloqueados;

22.12. Gerar histórico dos Top Level 10 (dez) "bloqueados" com o total das detecções, das ameaças e aplicativos;

23. RELATÓRIO E GRÁFICOS GERAIS DO TRÁFEGO IPS

23.1. Gerar gráficos estatísticos do tráfego IPS contendo as seguintes informações: total de ataques detectados, total de ataques bloqueados;

23.2. Gerar gráfico, histórico ou resumo diário, do total de trafego IPS da relação de eventos entre os "ataques detectados" e os "ataques bloqueados" no intervalo de tempo de 1 (uma) hora;

23.3. Gerar gráfico, histórico ou resumo mensal, do total de trafego IPS da relação de eventos entre os "ataques detectados" e dos "ataques bloqueados" no intervalo de tempo de 1 (hum) dia;

23.4. Gerar gráficos estatísticos do tráfego IPS contendo as informações do total dos ataques detectados por grau de risco e impacto na rede, mínimo de 3 (três) tipos de graus de risco ou impacto;

23.5. Gerar gráficos, históricos ou resumos diários, do total de tráfego IPS dos ataques detectados por grau de risco e impacto na rede, mínimo de 3 (três) tipos de graus de impacto no intervalo de tempo de 1 (uma) hora;

23.6. Gerar gráficos, históricos ou resumos mensais, do total de tráfego IPS dos ataques detectados por grau de risco e impacto na rede, mínimo de 3 (três) tipos de graus de impacto no intervalo de tempo de 1 (hum) dia;

23.7. Gerar histórico dos Tops 10 (dez) "ataques detectados", com o total de detecções e o tipo de risco ou impacto na rede;

23.8. Gerar histórico dos Top Level 10 (dez), inclusive a relação de eventos entre os "ataques" e os "endereços IP ou usuários" com o tipo de risco ou impacto na rede, total de detecções e o total de bloqueados, com a opção de ordenação por detecções e bloqueados;

23.9. Gerar histórico dos Top Level 10 (dez), inclusive a relação de eventos entre o "grau de risco" e os "endereços IP ou usuários" com o total de detecções e o total de bloqueados, com a opção de ordenação por detecção e bloqueados;

23.10. Gerar histórico dos Tops Level 10 (dez), "categorias de ataques" com o total das detecções e total de bloqueados, com a opção de detalhar a categoria e identificar os endereços IPs ou usuários atacantes;

24. SERVIÇO DE INSTALAÇÃO

24.1. Para as soluções ofertadas, a contratada deverá cotar um valor total para a instalação e customização inicial dos dispositivos adquiridos, dimensionado um banco de horas de XX horas para as atividades de ativação das soluções firewall UTM e firewall de e-mail;

24.2. Este serviço deverá ser utilizado para a operacionalização inicial dos produtos adquiridos, customização, funcionalidades e políticas;

24.3. A instalação deve ser feita por técnicos treinados e certificados, comprovados através de atestado emitido pelo fabricante;

24.4. Toda a despesa de deslocamento e hospedagem deve ser de responsabilidade da contratada;

25. SERVIÇOS DE PRESTAÇÃO DE SUPORTE TÉCNICO REMOTO 14x6

25.1. Serviço de suporte REMOTO para os equipamentos de segurança de borda contratados, no horário comercial (Segunda-feira a Sábado de 08h às 22h), pelo tempo de contrato, com as seguintes características: A

contratada deve possuir serviço de abertura de chamados remoto capaz de abrir chamados de forma centralizada, em caso de ocorrências de defeitos e/ou falhas na rede relativos aos equipamentos e/ou produtos fornecidos;

25.2. A contratada deverá iniciar o atendimento de suporte em no máximo 8 horas úteis após a abertura do chamado;

25.3. A contratada deverá fornecer atestado comprovando a existência de equipe técnica de no mínimo 3 pessoas capacitadas em todas as soluções adquiridas. O atestado deverá ser fornecido pelo fabricante;

25.4. A CONTRATADA será eximida da aplicação das sanções administrativas para os respectivos chamados em que sejam descumpridos os tempos de solução, desde que comprovadas as seguintes situações: Quando constatado que o problema está relacionado a "bug" no produto e que o fabricante não possui uma correção imediata para tal, sendo este fato declarado pelo próprio;

25.5. A CONTRATADA tomou todas as medidas possíveis visando providenciar solução de contorno;

26. TABELA PARA FORMAÇÃO DE PREÇO DO PRODUTO FORNECIDO

ITEM	DESCRIÇÃO	QDE
4	FIREWALL UTM: APPLIANCE PARA SOLUÇÃO DE SEGURANÇA UTM DE 1.000 MBPS DE CAPACIDADE DE FIREWALL – Para 12 meses	01
26	BANCO DE HORAS PARA EXECUÇÃO DE SERVIÇO ESPECIALIZADO DE CONSULTORIA, IMPLEMENTAÇÃO, TREINAMENTO (PACOTE DE 08 HORAS)	03
27	SERVIÇO MENSAL DE PRESTAÇÃO DE SUPORTE TÉCNICO REMOTO 14X6, EM HORAS	05

3 – JUSTIFICATIVA

A contratação de empresa especializada na implantação de sistema de controle de uso de internet na Câmara Municipal de Taboão da Serra é de suma importância para segurança de todo trafego de dados, tais como; software integrado com firewall, filtro de conteúdo de Internet, AntiSpam e E-mail.

Diante disso, a implantação do serviço se justifica pela necessidade de garantir a adequada proteção no acesso, evitando e prevenindo fontes de furto de dados e ameaças, em ambientes heterogêneos e distribuídos, bem como efetivação de ações corretivas.

ANEXO II
PROPOSTA DE PREÇO
PAPEL TIMBRADO DA EMPRESA

A
Câmara Municipal de Taboão da Serra
Setor de Licitações

Objeto: Contratação de empresa especializada na prestação de serviços de implantação de sistema de segurança da informação, composta por hardware e software em toda a rede de dados da Câmara Municipal de Taboão da Serra.
Convite nº ___/2017
Processo nº ___/2017

Empresa Proponente:
Endereço: **Bairro:** **Cidade:** **U.F.:**
CEP: **C.N.P.J./M.F.:**
Tel.: **Fax./e-mail:**

Apresentamos a Câmara Municipal de Taboão da Serra, nossa proposta de preço conforme ao que segue.

ITEM ÚNICO	
Preço para a implantação de sistema de segurança da informação, composta por hardware e software em toda a rede de dados da Câmara Municipal de Taboão da Serra, em moeda corrente nacional, em algarismo e por extenso >>>>>>>	**R$ ....** **.....)**
TOTAL GERAL GLOBAL	**R$ ....** **(.....)**

Validade da proposta: 60 (sessenta) dias.
Condições de pagamento: conforme edital.

Cidade, ____ de _____ de 2017.

Nome Representante legal:
R.G.:

Anexo III – Minuta do Contrato

Contrato nº 45/2017 - Processo nº 45/2017 – Convite 36/2017

Contratante: Câmara Municipal de Taboão da Serra.

Contratada:

Objeto: Contratação de empresa especializada na prestação de serviços de implantação de sistema de segurança da informação, composta por hardware e software em toda a rede de dados da Câmara Municipal de Taboão da Serra.

Aos ___ dia do mês de _____ do ano de 2017, pelo presente instrumento e na melhor forma de direito. Os abaixo-assinados, de um lado na qualidade de **CONTRATANTE** a **CÂMARA MUNICIPAL DE TABOÃO DA SERRA**, inscrito no CNPJ/MF sob o nº 60.547.841/0001-45, São Paulo, sito a Estrada São Francisco, nº 2013, Jardim Wanda, Taboão da Serra, São Paulo, através de sua Presidente, **JOICE MARQUES DA SILVA**, e de outro lado na qualidade de **CONTRATADA** à empresa, _____, com sede à _____, com CNPJ/MF Nº _____, neste ato representado pelo Sr. _____, portador da cédula de identidade RG nº _____, inscrito no CPF/MF sob nº _____, que assinam o presente relativo à contratação de empresa especializada na prestação de serviços de implantação de sistema de segurança da informação, composta por hardware e software em toda a rede de dados da Câmara Municipal de Taboão da Serra sobre as cláusulas e condições seguintes:

CLÁUSULA 1º - DO OBJETO

O presente instrumento é celebrado e regido com base na Lei Federal 8.666/93, atualizada pela Lei Federal 8.883/94, tem por objeto à contratação de empresa especializada na prestação de serviços de implantação de sistema de segurança da informação, composta por hardware e software em toda a rede de dados da Câmara Municipal de Taboão da Serra, cuja execução será regida pelas cláusulas deste instrumento que é lavrado nos termos da proposta oferecida pela **CONTRATADA** no **Convite ___/2017**, cujo teor ora é ratificado e que, rubricado pelas partes, passa a fazer parte integrante deste contrato.

A CONTRATADA deverá realizar os seguintes serviços:

1. Implantação do sistema de segurança da informação com solução integrada de Firewall NEXT GENERATION, composta de Hardware e Software de segurança da informação do tipo UTM (Unified Threat Management), entendendo-se como tais o conjunto de serviços e recursos de: Filtro de pacotes com controle de estado, Filtro de conteúdo web, Interceptação SSL, Filtro de aplicações, Controle da web 2.0, Inspeção com proteção contra ataques de Malwares, vírus, worm, e aplicativos maliciosos, integrar soluções do tipo (IDS/IPS, ATP,

QoS, Balanceamento de serviços, Redundância de links, VPN, DHCP e DNS). Com a capacidade de integrar todos os recursos em um único dispositivo.

A CONTRATADA deverá cumprir os seguintes critérios:

1. Implantação de servidor Appliance de UTM de 1000 Mbps de capacidade de firewall com garantia e atualização para 12 meses;
2. A solução de firewall deverá ser integrada com tecnologia de proteção de rede stateful packet inspection, serviços e recursos modulares de Filtro de conteúdo web, Interceptação SSL, Controle da web 2.0, Inspeção com proteção contra ataques de malwares, vírus, worms e aplicativos maliciosos (IDS/IPS), QoS, VPN e Filtro de aplicações;
3. APL UTM BB; Software License e UTM Subscription Advance;
4. Instalação e treinamento técnico dos servidores/usuários.
5. Comunicar à Fiscalização e proceder, às suas expensas, as correções necessárias, sempre que ocorrerem falhas, erros ou omissões na execução do serviço, especificações e demais elementos técnicos que integram este Edital, assumindo a responsabilidade pela correta execução de todos os serviços. Tais correções somente serão efetuadas com a aprovação da Fiscalização.
6. Reparar ou corrigir, total ou parcialmente, às suas expensas, serviços objetos do presente contrato em que se verifiquem vícios, defeitos ou incorreções, resultantes de execução irregular, do emprego de materiais ou equipamentos inadequados ou não correspondentes às especificações.

CLÁUSULA 2° - DO PRAZO

O prazo para implantação dos sistemas e serviços ora contratados será de 15 (quinze) dias corridos a contar da data da assinatura do contrato, podendo eventualmente ser prorrogado, quando devidamente justificado o motivo, nos termos do artigo 57 da Lei Federal 8.666/93, atualizada pela Lei 8.883/94.

CLÁUSULA 3° - DO PREÇO E DAS CONDIÇÕES DE PAGAMENTO

3.1 – Pela prestação de serviços a **Contratante** pagará a **Contratada** o valor único de R$ _____ (_____), pela totalidade da execução do serviço, em moeda corrente do País.
3.2 – No valor ofertado estão inclusas todas as despesas diretas e indiretas, bem como os impostos incidentes, ficando certo de que à Câmara Municipal nenhum outro ônus caberá além do pagamento do preço constante neste contrato.
3.3 – O pagamento será efetuado no prazo de até 05 (cinco) dias, após a implantação do sistema, devidamente comprovados pelo responsável direto em sua Divisão de Tesouraria, situada à Estrada São Francisco, 2013, Jd. Wanda, Taboão da Serra/SP, CEP 06765-001, mediante a apresentação da Nota Fiscal dos Serviços.

Parágrafo Único – os pagamentos efetuados em desacordo com os prazos estipulados serão corrigidos monetariamente, desde a data do vencimento até a data do efetivo pagamento da obrigação, nos termos da legislação vigente.
3.6 – A Contratante não remunerará a Contratada quando do não cumprimento, sem a devida justificativa de atraso da execução do serviço.
3.7 – Os valores a serem pagos não poderão ser reajustados, pois se trata de período não superior a 01 (um) ano, conforme previsto em Lei.

CLÁUSULA 4º - DOS RECURSOS ORÇAMENTÁRIOS

As despesas decorrentes da execução da presente licitação onerarão a seguinte dotação: 3.3.90.39.00 do orçamento vigente.

CLÁUSULA 5º - DAS OBRIGAÇÕES DA CONTRATANTE.

5.1 – Constituem responsabilidade da CMTS:

a) Fiscalizar a qualidade dos serviços prestados, determinando, se necessário, a reparação, correção, remoção, reconstituição ou substituição, às expensas da Contratada, dos serviços que tenham vícios, defeitos ou incorreções resultantes da execução do serviço;
b) Informar com 01(um) dia de antecedência a possível modificação de datas e/ou horários dos eventos.

CLÁUSULA 6º - DAS OBRIGAÇÕES DA CONTRATADA.

6.1 – Constituem responsabilidades da licitante vencedora:

a) Executar os serviços descritos no Termo de Referência e Anexo I deste Convite, em conformidade com as condições nele estabelecidas;
b) Zelar pela qualidade dos serviços;
c) Providenciar a imediata correção das deficiências e/ou irregularidades apontadas pelo setor responsável da C.M.T.S;
d) Manter, durante a execução do objeto deste Convite, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;
e) Uso adequado de equipamentos de proteção individual (EPIs), quando aplicável.

CLÁUSULA 7º - DAS INCIDÊNCIAS FISCAIS.

A **Contratada** é responsável por todos os ônus e obrigações de origem fiscal, trabalhista, previdenciária, tributária, securitária, civil e comercial decorrentes de sua prestação de serviço ora contratado.

CLÁUSULA 8º - DAS MULTAS E RESPONSABILIDADES.

No caso de ocorrer inexecução total ou parcial do presente contrato, ou de sua rescisão por parte da **Contratada**, ser-lhe-ão aplicadas às sanções administrativas na Lei Federal nº 8666/93, atualizada pela Lei Federal 8.883/94, que seguem:
8.1 - advertência;
8.2 - multa nos termos previstos na Lei Federal 8666/93, atualizada pela Lei Federal 8883/94;
8.3 - multa de 10% (dez por cento) por inexecução parcial do contrato, o qual incidirá sobre o valor total do contrato, devidamente reajustado na data do efetivo pagamento da multa;
8.4 – multa de 30% (trinta por cento) por inexecução total do contrato, ou recusa em assinar o mesmo, a qual incidirá sobre o valor total do contrato, devidamente reajustado na data do efetivo pagamento da multa;
8.6 - suspensão temporária de participar de licitação e impedimento de contratar com a Administração por prazo superior a 02 (dois) anos;
8.7 - declaração de inidoneidade para licitar ou contratar com a Administração, enquanto perdurarem os motivos da punição ou até que seja promovida a reabilitação, perante a autoridade que aplicou a penalidade;
8.8 – a aplicação das multas é independente da aplicação das demais sanções.

CLÁUSULA 9º - DA RESCISÃO.

Este contrato poderá ser rescindido, unilateralmente, de pleno direito, independentemente de interpelação judicial, caso ocorra qualquer das hipóteses previstas pelo artigo 79 I, da Lei Federal nº 8666/93, atualizada pela Lei Federal 8.883/94, ou por acordo entre as partes, ou ainda judicialmente, nos termos da legislação.

CLÁUSULA 10º - DA CESSÃO OU TRANSFERÊNCIA DO CONTRATO.

O presente contrato não poderá ser objeto de cessão ou transferência, no todo ou em parte.

CLÁUSULA 11º - DA FORÇA MAIOR OU DO CASO FORTUITO.

Nenhuma das partes será considerada inadimplente no cumprimento de suas obrigações caso haja ocorrência de eventos que, por sua natureza ou abrangência, possam ser caracterizados como fortuito ou força maior.

CLÁUSULA 12º - DO FORO.

Fica eleita a Comarca de Taboão da Serra para dirimir quaisquer dúvidas decorrentes do presente contrato.

E por estarem justas e acordadas, assinam o presente contrato em 3 (três) vias de igual forma e teor na presença das testemunhas abaixo para que produza seus efeitos jurídicos.

Taboão da Serra, ___ de _____ de 2017.

JOICE MARQUES DA SILVA
CÂMARA MUNICIPAL DE TABOÃO DA SERRA
CONTRATANTE

CONTRATADA

Testemunhas:

1ª)

2ª)

ANEXO IV – DECLARAÇÃO EPP-ME

MODALIDADE: CONVITE

Nº 36/2017

PROCESSO Nº 45/2017

Objeto: Contratação de empresa especializada na prestação de serviços de implantação de sistema de segurança da informação, composta por hardware e software em toda a rede de dados da Câmara Municipal de Taboão da Serra.

DECLARAÇÃO DE QUE ESTÁ ENQUADRADA COMO MICROEMPRESA OU EMPRESA DE PEQUENO PORTE NOS TERMOS DO ARTIGO 3º DA LEI COMPLEMENTAR Nº 123/2006, CASO SE ENQUADRE NOS TERMOS DESSA LEGISLAÇÃO MAIS BENÉFICA.

(PAPEL TIMBRADO DA EMPRESA LICITANTE – APRESENTAÇÃO OBRIGATÓRIA PARA TODAS AS LICITANTES)

A_____ (nome da licitante) _____, qualificada como microempresa (ou empresa de pequeno porte) por seu representante legal (doc. Anexo), inscrita no CNJP sob nº _____, com sede à _____, declara para os devidos fins de direito que está enquadrada como Microempresa - Me ou Empresa de Pequeno Porte - EPP, nos termos do artigo 3º da Lei Complementar nº 123, de 14 de dezembro de 2006. Sendo expressão da verdade, subscrevo-me.

Taboão da Serra, _____ de _____ de 2017.

_____

(assinatura e identificação do responsável legal/procurador da licitante)
Nome:
R.G.:
Cargo:

ORÇAMENTO ESTIMATIVO

PROCESSO Nº 45/2017
Convite nº36/2017

OBJETO: Contratação de empresa especializada na prestação de serviços de implantação de sistema de segurança da informação, composta por hardware e software em toda a rede de dados da Câmara Municipal de Taboão da Serra.

			QTDE	Mattos Sistemas		INFOPROTECT		FORTICS TECNOLOLIGIA		valor medio	valor medio
Item	Produtos	Unid.	ESTIMADA	Valor Unitário	Subtotal	Valor Unitário	Subtotal	Valor Unitário	Subtotal	unitário	total
1	Contratação de empresa especializada na prestação de serviços de implantação de sistema de segurança da informação, composta por hardware e software em toda a rede de dados	Unid.	1	R$ 74.900,00	R$ 74.900,00	R$ 79.350,00	R$ 79.350,00	R$ 76.900,00	R$ 76.900,00	R$ 77.050,00	R$ 77.050,00
					R$ 74.900,00		R$ 79.350,00		R$ 76.900,00		R$ 77.050,00
	Média Estimada - de R$ 77.050,00 (setenta e sete mil e cinquenta reais)										

CÂMARA MUNICIPAL TABOÃO DA SERRA SP

Folha nº 145
Proc. 10/2017

ANEXO VI
(TIMBRE DA EMPRESA)

DECLARAÇÃO DE QUALIFICAÇÃO TÉCNICA

A Empresa , inscrita no CNPJ: 00.000.000/0000-00, estabelecida sito à Rua , nº , Bairro, Cidade, Estado, CEP, neste ato representada por seu titular o (a) Sr.(a), nacionalidade, estado civil, profissão, número do documento RG nº e do CPF: , residente e domiciliado sito à Rua , nº , Bairro, Cidade, Estado, CEP, DECLARA para os devidos fins que o Sr.(a) , portador do RG nº e do CPF , desempenha nesta a empresa a função de _____ desde_____, estando apto para execução do serviço contratado. (Implantação de sistema de segurança da informação, composta por hardware e software em toda a rede de dados da Câmara Municipal de Taboão da Serra).

Para maior clareza, firmo o presente sob as penas da lei.

Cidade, de de 2017

_____
Empresa
CNPJ:
Representante
RG:

ANEXO VII – Atestado de Visita Técnica

Convite nº ____/2017- Processo nº ____/2017

ATESTADO DE VISITA TÉCNICA

Atestamos que a empresa _____, representada por seu(representante, sócio, proprietário) _____, portador do RG _____, cargo _____, visitou a unidade de execução do serviço pertinente ao convite nº _____, objeto: **Serviços de implantação de sistema de segurança da informação, composta por hardware e software em toda a rede de dados da Câmara Municipal de Taboão da Serra.**

Taboão da Serra,_____ de _____ de 2017.

_____
Reinaldo Silva Borges
Chefe de Compras, Licitações e Contratos

_____
(assinatura e identificação do responsável legal/procurador da licitante)
Nome:
R.G.:
Cargo:

Estrada São Francisco, 2013 – Jd. Wanda – CEP 06765-001 - Taboão da Serra – SP – Fone/Fax: 4788-9300.
Visite o site da Câmara – http://www.camarataboao.sp.gov.br

Folha nº 152
Proc. 45/2017

RECIBO DE ENTREGA

CONVITE N° 36/2017.
PROCESSO N° 45/2017.

EMPRESA: _____

Convidamos essa empresa para participar da Licitação, na modalidade Convite do tipo MENOR PREÇO GLOBAL, nos termos da Lei Federal 8.666/93, atualizada pelas Leis n°8.883/94, 9.032/95 e 9.648/98, e demais disposições regulamentares, objetivando contratação de empresa especializada na prestação de serviços de implantação de sistema de segurança da informação, composta por hardware e software em toda a rede de dados da Câmara Municipal de Taboão da Serra, conforme Edital, que segue a este.

Os envelopes contendo as propostas de preços e documentos de habilitação deverão ser entregues na Estrada São Francisco, nº2013, Térreo, Jd. Wanda, Taboão da Serra, SP, no setor de Licitações, até o dia 11 de outubro de 2017, às 14h30min.

No dia 11 de outubro de 2017, às 14h30min, em sessão pública, a ser realizada no mesmo endereço, se dará à abertura dos mesmos pela Comissão de Licitações. Não serão considerados os envelopes entregues com atraso.

Taboão da Serra, ____ de _____ de 2017.

Reinaldo da Silva Borges
Chefe de Compras, Licitações e Contrato

Declaro que recebi nesta data cópia do convite 36/2017, Processo 45/2017.

Nome:

Assinatura _____

Telefone da Empresa

Carimbo da Empresa com CNPJ.

CÂMARA MUNICIPAL TABOÃO DA SERRA