ANEXO IV– COMPROVAÇÃO DOS REQUISITOS TÉCNICOS				
Descrição do item	**Atende Especificação (Sim ou Não)**	**Nome do Manual/Datasheeet**	**Referência detalhada (indicar o tipo/nome do documento, página(s) e seção(ões) que comprova(m) o atendimento da especificação**	**Para uso exclusivo da CONTRATANTE. Atende? (SIM/NÃO)**
ITEM 01 - ESPECIFICAÇÕES TÉCNICAS DOS APPLIANCES VPN				
1 CARACTERÍSTICAS GERAIS DOS APPLIANCES VPN (VIRTUAL PRIVATE NETWORK, REDE PARTICULAR VIRTUAL):				
1.1 Composição da solução:				
1.1.1 A solução de appliances Firewall/VPN a ser contratada é composta do fornecimento de equipamentos, bem como a garantia e suporte técnico do fabricante pelo período de 36 (trinta e seis) meses.				
1.1.2 A solução deverá possuir interoperabilidade com a solução de VPN em utilização no TJCE;				
1.1.3 A solução deverá estar licenciada para desempenhar as funcionalidades de firewall e VPN, com suporte de garantia pelo período de 36 (trinta e seis) meses;				
1.1.4 Todas as licenças/ativações devem ser do tipo perpétua, ou seja, continuarão sendo de propriedade do TJCE após o suporte de garantia de 3 (três) anos. Continuarão funcionando sem perda de performance após o suporte de 3 (três) anos.				
1.1.5 Todos os appliances deverão atender aos requisitos mínimos de funcionalidades:				
1.1.5.1 Solução em appliance de Firewall stateful packet inspection. Não serão aceitas soluções baseadas em PC de uso geral ou soluções que contenham componentes do tipo acionadores de discos rígidos ou flexíveis;				
1.1.6 Fornecer suporte a VPN IPSec, incluindo criptografia DES-56 bits, 3DES-168 bits, AES-128, AES-192 e AES-256, com capacidade de implementar topologias site-to-site e client-to-site;				
1.1.7 Possuir recursos capazes de detectar e evitar automaticamente ataques de DDoS, também, dentro dos tuneis VPN IPSEC;				
1.1.8 Implementar recurso de NAT (Network Address Translation) tipo one-to-one, many-to-one, e tradução simultânea de endereço IP, porta TCP de conexão (NAPT), e NAT transversal em VPN IPSec;				
1.1.9 Possuir servidor de DHCP (dynamic host configuration protocol) interno com capacidade de alocação de endereçamento IP para as estações conectadas às interfaces do firewall e em VPN;				
1.1.10 Possibilitar a aplicação de regras de firewall por IP e grupo de usuários, permitindo a definição de regras para determinado horário ou período (dia da semana e hora) com matriz de horários que possibilite o bloqueio de serviços em horários específicos, tendo o início e fim das conexões vinculadas a essa matriz de horários;				
1.1.11 Possuir mecanismo que limite o número máximo de conexões simultâneas de uma mesma origem a um determinado serviço ou a um determinado servidor e que possa ser aplicado individualmente para cada regra de filtragem;				
1.1.12 Possuir validação completa da sintaxe de toda sinalização de VoIP e pacotes de streams de mídia (para assegurar que pacotes mal-formados não possam passar pelo firewall e afetar adversamente o destinatário da comunicação);				
1.1.13 Suportar o registro do firewall dinamicamente, pelo seu endereço IP de WAN, num provedor de serviços de DDNS;				
1.1.14 Suportar endereçamento na interface de WAN por PPPOE (Point-to-point Protocol Over Ethernet), IP estático e dinâmico e por DHCP;				
1.1.15 Permitir alta disponibilidade das interfaces WAN nas modalidades ativo-ativo (balanceamento) e ativo-passivo (redundância);				
1.1.16 Permitir a definição de objetos como grupo de usuários, redes ou serviços de modo que, quando a política de segurança mudar, o administrador possa modificar o objeto pré-definido e propagar as mudanças instantaneamente sem necessidade de redefinir as regras;				
1.1.17 Possuir gerenciamento de banda de entrada e saída, suporte classes de serviço por DSCP (differentiated services code points);				
1.1.18 Possuir recurso de balanceamento de links WAN, com regras de balanceamento por conexão utilizando a métrica round-robin e funcionalidade de escoamento de tráfego para a interface WAN secundária;				
1.1.19 Possuir mecanismo que possibilite o funcionamento transparente dos protocolos FTP, SIP e H.323, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro;				
1.1.20 Possuir suporte ao protocolo SNMP, através de MIB2;				
1.1.21 Possuir a funcionalidade de hardware-failover ativo/passivo;				
1.2 Autenticação:				
1.2.1 Permitir a autenticação dos usuários utilizando servidores LDAP, AD e RADIUS;				
1.2.2 Permitir o cadastro manual dos usuários e grupos diretamente no firewall por meio da interface de gerência remota do equipamento;				
1.2.3 Permitir a integração com qualquer autoridade certificadora emissora de certificados X. 509 que siga o padrão de PKI descrito na RFC 2459;				
1.2.4 Permitir a atribuição de perfil por faixa de endereço IP nos casos em que a autenticação não seja requerida;				
1.2.5 Suportar padrão IPSec, de modo a estabelecer canais de criptografia com outros produtos que também suportem tal padrão;				
1.2.6 Suportar a criação de túneis seguros sobre IP (IPSec tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet;				
1.3 Administração				
1.3.1 A interface gráfica deverá possuir assistentes para facilitar a configuração inicial e administração do Firewall;				
1.3.2 Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o Firewall, com no mínimo dois níveis de permissão: total e apenas leitura;				
1.3.3 Possuir mecanismo para aplicar remotamente, pela interface gráfica, correções e atualizações para o Firewall;				

1.3.4 Possuir mecanismo para realizar remotamente, pela interface gráfica, cópias de segurança (backup) e restauração, sem a necessidade de se reinicializar o sistema (no caso de realização de backups);				
1.3.5 Permitir a visualização e o gerenciamento em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do Firewall, por serviços e endereços IP de origem e destino;				
1.3.6 Permitir a visualização, em forma gráfica, do percentual do uso de CPU e quantidade de tráfego de rede em todas as interfaces do Firewall, em tempo real;				
1.3.7 Permitir a visualização em tempo real, das políticas com maior tráfego e os endereços IPs mais acessados;				
1.3.8 Possibilitar o controle do tráfego, pelos endereços de origem e destino da comunicação;				
1.3.9 Possuir suporte a roteamento RIP e OSPF;				
1.3.10 Possuir interface orientada a linha de comando para a administração do firewall a partir do console ou conexão SSH;				
1.4 Log				
1.4.1 Possuir suporte a LOG via Syslog;				
1.4.2 Possibilitar o registro da comunicação realizada através do Firewall, sob demanda do administrador, das conexões abertas e das conexões recusadas pelo mesmo;				
1.4.3 Prover mecanismo(s) de consulta às informações registradas;				
1.4.4 Possibilitar a análise dos seus registros (LOGs) por, pelo menos, um programa analisador de LOG disponível no mercado;				
1.4.5 Possuir mecanismo que permita inspecionar o tráfego de rede em tempo real (sniffer) via interface gráfica, possibilitando exportar os dados visualizados para arquivo formato PCAP e permitindo a filtragem dos pacotes por protocolo, endereço IP de origem, endereço IP de destino, porta TCP de origem e porta TCP de destino;				
1.4.6 Permitir a visualização do tráfego de rede em tempo real nas interfaces de rede do Firewall;				
1.4.7 Não serão aceitas soluções baseadas em redirecionamento de tráfego para dispositivos externos ao Firewall para análise de arquivos ou pacotes de dados.				
1.5 Elétricos:				
1.5.1 Possuir fonte de alimentação operando nas tensões 110/220V, com seleção automática de voltagem, e frequência de 50/60Hz.				
1.6 Físicos:				
1.6.1 Todos os equipamentos entregues deverão ser novos e sem uso prévio, devendo estar em linha de produção.				
1.7 Requisitos Específicos dos Appliances Vpn:				
1.7.1 Todos os appliances deverão atender aos requisitos mínimos de performance:				
1.7.1.1 Possuir, no mínimo, 3 (três) interfaces Gigabit Ethernet 10/100/1000;				
1.7.1.2 Possuir, no mínimo, 1 (uma) interface padrão USB;				
1.7.1.3 No mínimo 200 usuários autenticados simultaneamente;				
1.7.2 Possuir performance de, e está licenciado para:				
1.7.2.1 Licenciamento perpétuo sem perda de performance após garantia do fabricante;				
1.7.2.2 49.000 (quarenta e nove mil) conexões TCP/IP simultâneas;				
1.7.2.3 Implementar 2.000 (duas mil) novas conexões TCP/IP por segundo;				
1.7.2.4 Firewall stateful inspection de 400 Mbps (quatrocentos megabits) por segundo para tráfego TCP;				
1.7.2.5 VPN IPSec (3DES/AES) 100 Mbps (cem megabits) por segundo para tráfego TCP.				
2 SOFTWARE DE GERÊNCIA				
2.1 Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de 5 equipamentos do ITEM 1.				
2.2 O restante do licenciamento para gerenciamento dos equipamentos deve ser divido por pacotes de licenças de 10 unidades de equipamentos, perfazendo 10 pacotes de licenças.				
2.3 Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções.				
2.4 O gerenciamento centralizado poderá ser entregue como appliance físico ou appliance virtual ou Software compatível com Windows ou Linux. Caso seja entregue em appliance fisíco deve ser compatível com rack 19 polegadas e possuir todos acessórios necessários para sua instalação. Caso seja entregue em appliance virtual dever ser compatível com VMware ESX;				
2.5 Deve permitir controle global de políticas para todos os equipamentos que compõe a plataforma de segurança;				
2.6 Deve suportar organizar os dispositivos administrados em grupos;				
2.7 Deve implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de firewalls;				
2.8 Deve consolidar logs e relatórios de todos os dispositivos administrados;				
2.9 Deve permitir que a configuração ou políticas dos firewalls seja importada na plataforma de gerenciamento centralizado e que possa ser usada em outros firewalls e grupos de firewalls;				
2.10 Deve mostrar os status dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado;				
2.11 Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;				
2.12 O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) ou API aberta;				
2.13 Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows;				
2.14 O gerenciamento deve permitir/possuir:				

2.14.1 Criação e administração de políticas de firewall e controle de aplicação;				
2.14.2 Criação e administração de políticas de IPS e Antivírus;				
2.14.3 Criação e administração de políticas de Filtro de URL;				
2.14.4 Monitoração de logs;				
2.14.5 Debugging;				
2.14.6 Captura de pacotes; e				
2.14.7 Acesso concorrente de administradores;				
2.15 Deve possuir mecanismo de busca na solução onde possa se consultar por uma string tais como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPS;				
2.16 Deve permitir usar palavras chaves para facilitar identificação de regras;				
2.17 Autenticação integrada ao Microsoft Active Directory ou servidor Radius;				
2.18 Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;				
2.19 Deve atribuir sequencialmente um número a cada regra de firewall;				
2.20 Criação de regras que fiquem ativas em horário definido;				
2.21 Backup das configurações e rollback de configuração para a última configuração salva;				
2.22 Habilidade de upgrade via SCP ou TFTP ou interface de gerenciamento;				
2.23 Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors);				
2.24 Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;				
2.25 Deve ser possível exportar os logs em CSV;				
2.26 Deve permitir que os logs e relatórios sejam expurgados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado;				
2.27 Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. IP's distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;				
2.28 Gerar alertas automáticos via:				
2.28.1 Email;				
2.28.2 Syslog.