TERMO DE REFERÊNCIA PARA CONTRATAÇÃO DE PRODUTOS/SERVIÇOS

A Confederação Brasileira de Voleibol - CBV

Torna público Termo de Referência para contratação de produtos/serviços, conforme escopo descrito abaixo:

NÚMERO DA SOLICITAÇÃO: 007502

LOCAL DE ENTREGA: CBV - RIOCENTROAv. Salvador Allende 6.555/ Pavilhão 1, entrada portão B,Riocen

DATA DE ENTREGA: 24/05/2017

==========

MATERIAL DE INFORMÁTICA

Aquisição de equipamento 1(UM) firewalll para o escritório do Riocentro, conforme especificações tecnicas.

1. ESPECIFICAÇÕES GERAIS
1.1 Aquisição de Firewalls Appliance (hardware dedicado) com throughput de no mínimo 1 Gbps, incluindo sistema de segurança do tipo IDS (Intrusion Detection System), IPS (Intrusion Prevention System), IPS Performance 350 Mbps, suporte à adição de licença para filtro de conteúdo e gateway de antivírus e antispyware, bem como suporte instalação e assistência técnica especializada.
1.2 Aquisição de licenças de filtro de conteúdo e gateway antivírus/antispyware
1.3. Quantidade: 01 (UM)

2. ESPECIFICAÇÕES TÉCNICAS DO FIREWALL
2.1 Firewall appliance (hardware), baseado na tecnologia Stateful Packet Inspection com capacidade de Deep Packet Inspection para filtragem de tráfego IP, com funcionalidade de operação em modo de Alta Disponibilidade.;

2.2. Deve possuir, no mínimo, 2 (duas) interfaces de rede para conexão WAN, com velocidade de 10/100/1000 Mbps, autosense, compatíveis com os padrões IEEE 802.3i, IEEE 802.3u e IEEE 802.3ab;

2.3 Deve possuir no mínimo 08 (oito) interfaces de redes distintas, com velocidade de 10/100/1000 Mbps, autosense, compatíveis com os padrões IEEE 802.3i, IEEE 802.3u e IEEE 802.3ab;

2.4 Permitir a criação de, no mínimo, 500 VLAN, padrão IEEE 802.1Q, definindo interfaces virtuais por identificadores de VLAN (VLAN ID tag). As interfaces virtuais devem permitir as mesmas funcionalidades das interfaces físicas, incluindo designação de zona de segurança, servidores DHCP,

NAT, VPN e regras de controle de acesso

2.5 Deve possuir licenças e recursos de hardware, dimensionados para permitir a configuração de, no mínimo, 75 firewalls virtuais, possibilitando o gerenciamento de interfaces, VLAN, zonas, regras, rotas e VPN, de forma individualizada para cada firewalll;

2.6 Possuir performance de firewall Stateful Inspection de, no mínimo, 1 Gbps (throughput);

2.7 Possuir suporte a número ilimitado de endereços IP nas redes internas;

2.7 Permitir a implementação de no mínimo 2.000 policies;

2.9 Possuir capacidade para um mínimo de 100.000 conexões TCP/IP concorrentes e simultâneas;

2.10 Deverá permitir a configuração dos seguintes modos de operação: transparente mode, NAT mode e routing mode;

2.11 Permitir a criação de túneis VPN (Virtual Private Network) Site to Site e Client to Site sob os protocolos PPTP e IPSec. Deverão ser inclusas gratuitamente no mínimo 200 licenças para VPN Client to Site e 100 licenças Site to Site. Deverá ser fornecido software cliente VPN IPSec, do mesmo fabricante, compatível com o modelo ofertado e compatível com sistema operacional Windows 7 e Windows XP;

2.12 Possuir performance de VPN IPsec, por appliance de, no mínimo, 600 Mbps (throughput) bidirecional, com criptografia 3DES (168 bits) ou AES e pelo menos um túnel de VPN IPsec estabelecido

2.13 Implementar recurso de NAT (network address translation) do tipo um para um (one-to-one), um para muitos (one-to-many), muitos para um (many-to-one) e muitos para muitos (many-to-many) e tradução simultânea de endereço IP e porta TCP de conexão (NAPT);

2.14 Possuir suporte a NAT simétrico;

2.15 Suportar NAT em todas as interfaces;

2.16 Deverá possuir a função de TOLERANCIA A FALHAS (Alta Disponibilidade), nos modos Ativo/Passivo e/ou Ativo/Ativo, com todas as licenças de software habilitadas para tal, de forma a garantir que, se um dos firewalls parar de funcionar, o outro deverá assumir automaticamente, suportando todo o tráfego e processamento;

2.17 Possuir recurso habilitado incluso de IDS e IPS interno, capaz de detectar e evitar automaticamente (no mínimo), IP Source Spoofing, IP Source Routing, Tunel IPsec e ataques tipo DoS (DenialofService) como Ping of Death, SYN Flood, LAND Attack, IP Spoofing, com a possibilidade de se atualizar as assinaturas e carregar as novas, sem interrupção, através de atualização automática do software de sistema operacional do equipamento (appliance);

2.18 Deverão ser fornecidas licenças de IPS/IDS, incluindo licenças para updates, com atualização automática para o período contratado;

2.19 Possuir performance de IPS de, no mínimo, 750 Mbps (throughput);

2.20 Possibilitar o acesso via interface WEB, nos modos HTTP e HTTPS, para configuração e administração remota, inclusive via interface WAN, com total capacidade de administração sobre o sistema;

2.21 Suportar protocolo NTP para sincronismo de relógio do equipamento;

2.22 Suportar o protocolo SNMP, para checagem de status e TRAP para envio e notificação de alarmes;

2.23 Deve possuir suporte completo a protocolos de roteamento (rotas estáticas e dinâmicas OSPF, RIP e RIPv2), com possibilidade de programação de rotas para as interfaces;

2.24 Permitir a definição de rotas de tráfego baseadas em regras definidas por port de serviço (TCP/UDP) e endereço IP de origem ou destino;

2.25 Possibilitar a especificação de política por tempo, ou seja, permitir a definição de regras para determinado horário ou período (dia da semana e hora);

2.26 Deve possuir fonte de alimentação operando nas tensões 110/220 V, com seleção automática de voltagem e freqüência de 50/60 Hz;

2.27 Possuir estatística de utilização de CPU e memória do firewall;

2.28 Possibilitar a criação de entradas ARP estáticas para fixação de endereço IP com um número MAC específico;

2.29 Deverá permitir backup remoto de configuração;

2.30 Possuir função de DHCP Server e Client interno;

2.31 Capacidade de enviar e armazenar logs em um servidor remoto via protocolo syslog;

2.32 Deverá possuir função de debug online, com pesquisa por endereço IP (origem/destino) identificando no mínimo, informações do cabeçalho, porta e protocolo do pacote capturado;

2.33 Deverá ser fornecida a versão mais recente para todos os softwares internos dos equipamentos;

2.34 Suporte a ativação de filtro de conteúdo por URL (com atualização automática da base de dados, por palavra, categorias e no mínimo 40 categorias e filtro por grupos de usuários, que podem ser definidos por:

2.34.1 Contas de usuários em ambiente Active Directory;

2.34.2 Registros em base de dados LDAP, acessíveis sobre canal plain text ou sobre camada criptografada (SSL, TLS ou equivalente);

2.34.3. Endereços IP;

2.34.4. Os recursos de filtro de conteúdo serão opcionais, habilitados mediante a aquisição de licenças descritas no item 2.3;

2.35 Deverá suportar recursos de gateway de antivírus/antispyware atuando no tráfego da interface, no mínimo para os protocolos HTTP, SMTP, POP3, IMAP e FTP, com atualização automática e gratuita da base de dados Vírus.

2.35.1 Os recursos de gateway de antivírus/antispyware serão opcionais, habilitados mediante a aquisição de licenças descritas no item 2.3;

2.36. AntiSpyware:

2.36.1. Proibir downloads de spywares (incluindo downloads indesejados);

2.36.2. Bloquear acesso a sites de spywares ;

2.36.3. Detectar acessos de spywares a Internet ;

2.36.4. Facilitar a remoção de spywares ;

2.36.5. Inspeção de conteúdo .

2.36.6. Atualização automática e gratuita da base de dados.

2.37 Possuir suporte a IPv4 e IPv6 simultaneamente, com tradução de IPv4 para IPv6 e IPv6 para IPv4.

3. LICENÇAS DE FILTRO DE CONTEÚDO E GATEWAY ANITIVIRUS/ANTISPYWARE.
Quantidade: 01 (UM)
3.1. As licenças devem ser capazes de habilitar os recursos de filtro de conteúdo e gateway antivírus/antispyware descritas nos itens acima;

3.2. Deverão permitir atualização gratuita e automática;

3.3. Deverão permitir a utilização por número indefinido de usuários ou endereços IP;

3.4. Estão inclusos os serviços de instalação e configuração dos equipamentos, bem como serviços de suporte constante no edital;

3.5. As licenças deverão ser autossuficientes para cada aquisição, isto é, devem permitir a habilitação dos recursos sem que haja necessidade de novas aquisições;

3.6. As licenças deverão ser válidas por um prazo mínimo de 24 meses, com renovação automática ou por intermédio do fornecimento gratuito de novas licenças quando da expiração das mesmas;

4. ITENS GERAIS:
4.1 Kit para montagem em RACK de 19”.
4.2 Deverão ser fornecidos cabos de interconexão elétrica.

Atenção :

O PAGAMENTO DA NOTA FISCAL ESTÁ CONDICIONADO A ASSINATURA DA ORDEM DE COMPRAS, QUE DEVERÁ SER ENCAMINHADA JUNTAMENTE COM A NOTA FISCAL. "DE ACORDO COM A POLÍTICA DA CBV NÃO SERÃO ACEITOS BOLETOS EM NOME DE FACTORINGS OU DADOS BANCÁRIOS DE CNPJ DIFERENTE DO EMISSOR DA NOTA FISCAL."

INFORMAÇÃO SOBRE RETENÇÃO DE IMPOSTOS:

A CBV, em conformidade com as exigências impostas pela Receita Federal em sua Instrução Normativa "IN RFB 971/2009", realizará, nas notas fiscais de prestação de serviços envolvendo o uso de mão de obra, a retenção de 11% a título de INSS sobre o valor total da nota, caso não esteja especificado o valor da mão de obra e ainda a retenção de 1% sobre o valor da nota fiscal a título de retenção de imposto de renda, sendo a base de cálculo a mesma do INSS. Para notas fiscais não envolvendo serviços de mão de obra haverá a retenção de 1,5% de imposto de renda e, será recolhido ainda 4,65% (3%- COFINS + 0,65% PIS + 1% CSLL). Serão tratados individualmente os casos em que for necessário a retenção de ISS (variando entre 2% e 5% dependendo do município e atividade prestada).

A Confederação Brasileira de Voleibol - CBV

Torna público Termo de Referência para contratação de produtos/serviços, conforme escopo descrito abaixo:

NÚMERO DA SOLICITAÇÃO: 007503

LOCAL DE ENTREGA: CBV - SAQUAREMAAv
Salgado Filho, 7000 - Barra Nova - Saquarema
- RJCEP: 28990-

DATA DE ENTREGA: 20/05/2017

==========

MATERIAL DE INFORMÁTICA

Aquisição de equipamento 1(UM) firewalll para o escritório do Riocentro, conforme especificações tecnicas.

1. ESPECIFICAÇÕES GERAIS
1.1 Aquisição de Firewalls Appliance (hardware dedicado) com throughput de no mínimo 1 Gbps, incluindo sistema de segurança do tipo IDS (Intrusion Detection System), IPS (Intrusion Prevention System), IPS Performance 350 Mbps, suporte à adição de licença para filtro de conteúdo e gateway de antivírus e antispyware, bem como suporte instalação e assistência técnica especializada.
1.2 Aquisição de licenças de filtro de conteúdo e gateway antivírus/antispyware
1.3. Quantidade: 01 (UM)

2. ESPECIFICAÇÕES TÉCNICAS DO FIREWALL
2.1 Firewall appliance (hardware), baseado na tecnologia Stateful Packet Inspection com capacidade de Deep Packet Inspection para filtragem de tráfego IP, com funcionalidade de operação em modo de Alta Disponibilidade.;

2.2. Deve possuir, no mínimo, 2 (duas) interfaces de rede para conexão WAN, com velocidade de 10/100/1000 Mbps, autosense, compatíveis com os padrões IEEE 802.3i, IEEE 802.3u e IEEE 802.3ab;

2.3 Deve possuir no mínimo 08 (oito) interfaces de redes distintas, com velocidade de 10/100/1000 Mbps, autosense, compatíveis com os padrões IEEE 802.3i, IEEE 802.3u e IEEE 802.3ab;

2.4 Permitir a criação de, no mínimo, 500 VLAN, padrão IEEE 802.1Q, definindo interfaces virtuais por identificadores de VLAN (VLAN ID tag). As interfaces virtuais devem permitir as mesmas funcionalidades das interfaces físicas, incluindo designação de zona de segurança, servidores DHCP,

NAT, VPN e regras de controle de acesso

2.5 Deve possuir licenças e recursos de hardware, dimensionados para permitir a configuração de, no mínimo, 75 firewalls virtuais, possibilitando o gerenciamento de interfaces, VLAN, zonas, regras, rotas e VPN, de forma individualizada para cada firewalll;

2.6 Possuir performance de firewall Stateful Inspection de, no mínimo, 1 Gbps (throughput);

2.7 Possuir suporte a número ilimitado de endereços IP nas redes internas;

2.7 Permitir a implementação de no mínimo 2.000 policies;

2.9 Possuir capacidade para um mínimo de 100.000 conexões TCP/IP concorrentes e simultâneas;

2.10 Deverá permitir a configuração dos seguintes modos de operação: transparente mode, NAT mode e routing mode;

2.11 Permitir a criação de túneis VPN (Virtual Private Network) Site to Site e Client to Site sob os protocolos PPTP e IPSec. Deverão ser inclusas gratuitamente no mínimo 200 licenças para VPN Client to Site e 100 licenças Site to Site. Deverá ser fornecido software cliente VPN IPSec, do mesmo fabricante, compatível com o modelo ofertado e compatível com sistema operacional Windows 7 e Windows XP;

2.12 Possuir performance de VPN IPsec, por appliance de, no mínimo, 600 Mbps (throughput) bidirecional, com criptografia 3DES (168 bits) ou AES e pelo menos um túnel de VPN IPsec estabelecido

2.13 Implementar recurso de NAT (network address translation) do tipo um para um (one-to-one), um para muitos (one-to-many), muitos para um (many-to-one) e muitos para muitos (many-to-many) e tradução simultânea de endereço IP e porta TCP de conexão (NAPT);

2.14 Possuir suporte a NAT simétrico;

2.15 Suportar NAT em todas as interfaces;

2.16 Deverá possuir a função de TOLERANCIA A FALHAS (Alta Disponibilidade), nos modos Ativo/Passivo e/ou Ativo/Ativo, com todas as licenças de software habilitadas para tal, de forma a garantir que, se um dos firewalls parar de funcionar, o outro deverá assumir automaticamente, suportando todo o tráfego e processamento;

2.17 Possuir recurso habilitado incluso de IDS e IPS interno, capaz de detectar e evitar automaticamente (no mínimo), IP Source Spoofing, IP Source Routing, Tunel IPsec e ataques tipo DoS (DenialofService) como Ping of Death, SYN Flood, LAND Attack, IP Spoofing, com a possibilidade de se atualizar as assinaturas e carregar as novas, sem interrupção, através de atualização automática do software de sistema operacional do equipamento (appliance);

2.18 Deverão ser fornecidas licenças de IPS/IDS, incluindo licenças para updates, com atualização automática para o período contratado;

2.19 Possuir performance de IPS de, no mínimo, 750 Mbps (throughput);

2.20 Possibilitar o acesso via interface WEB, nos modos HTTP e HTTPS, para configuração e administração remota, inclusive via interface WAN, com total capacidade de administração sobre o sistema;

2.21 Suportar protocolo NTP para sincronismo de relógio do equipamento;

2.22 Suportar o protocolo SNMP, para checagem de status e TRAP para envio e notificação de alarmes;

2.23 Deve possuir suporte completo a protocolos de roteamento (rotas estáticas e dinâmicas OSPF, RIP e RIPv2), com possibilidade de programação de rotas para as interfaces;

2.24 Permitir a definição de rotas de tráfego baseadas em regras definidas por port de serviço (TCP/UDP) e endereço IP de origem ou destino;

2.25 Possibilitar a especificação de política por tempo, ou seja, permitir a definição de regras para determinado horário ou período (dia da semana e hora);

2.26 Deve possuir fonte de alimentação operando nas tensões 110/220 V, com seleção automática de voltagem e freqüência de 50/60 Hz;

2.27 Possuir estatística de utilização de CPU e memória do firewall;

2.28 Possibilitar a criação de entradas ARP estáticas para fixação de endereço IP com um número MAC específico;

2.29 Deverá permitir backup remoto de configuração;

2.30 Possuir função de DHCP Server e Client interno;

2.31 Capacidade de enviar e armazenar logs em um servidor remoto via protocolo syslog;

2.32 Deverá possuir função de debug online, com pesquisa por endereço IP (origem/destino) identificando no mínimo, informações do cabeçalho, porta e protocolo do pacote capturado;

2.33 Deverá ser fornecida a versão mais recente para todos os softwares internos dos equipamentos;

2.34 Suporte a ativação de filtro de conteúdo por URL (com atualização automática da base de dados, por palavra, categorias e no mínimo 40 categorias e filtro por grupos de usuários, que podem ser definidos por:

2.34.1 Contas de usuários em ambiente Active Directory;

2.34.2 Registros em base de dados LDAP, acessíveis sobre canal plain text ou sobre camada criptografada (SSL, TLS ou equivalente);

2.34.3. Endereços IP;

2.34.4. Os recursos de filtro de conteúdo serão opcionais, habilitados mediante a aquisição de licenças descritas no item 2.3;

2.35 Deverá suportar recursos de gateway de antivírus/antispyware atuando no tráfego da interface, no mínimo para os protocolos HTTP, SMTP, POP3, IMAP e FTP, com atualização automática e gratuita da base de dados Vírus.

2.35.1 Os recursos de gateway de antivírus/antispyware serão opcionais, habilitados mediante a aquisição de licenças descritas no item 2.3;

2.36. AntiSpyware:

2.36.1. Proibir downloads de spywares (incluindo downloads indesejados);

2.36.2. Bloquear acesso a sites de spywares ;

2.36.3. Detectar acessos de spywares a Internet ;

2.36.4. Facilitar a remoção de spywares ;

2.36.5. Inspeção de conteúdo .

2.36.6. Atualização automática e gratuita da base de dados.

2.37 Possuir suporte a IPv4 e IPv6 simultaneamente, com tradução de IPv4 para IPv6 e IPv6 para IPv4.

3. LICENÇAS DE FILTRO DE CONTEÚDO E GATEWAY ANITIVIRUS/ANTISPYWARE.
Quantidade: 01 (UM)
3.1. As licenças devem ser capazes de habilitar os recursos de filtro de conteúdo e gateway antivírus/antispyware descritas nos itens acima;

3.2. Deverão permitir atualização gratuita e automática;

3.3. Deverão permitir a utilização por número indefinido de usuários ou endereços IP;

3.4. Estão inclusos os serviços de instalação e configuração dos equipamentos, bem como serviços de suporte constante no edital;

3.5. As licenças deverão ser autossuficientes para cada aquisição, isto é, devem permitir a habilitação dos recursos sem que haja necessidade de novas aquisições;

3.6. As licenças deverão ser válidas por um prazo mínimo de 24 meses, com renovação automática ou por intermédio do fornecimento gratuito de novas licenças quando da expiração das mesmas;

4. ITENS GERAIS:
4.1 Kit para montagem em RACK de 19”.
4.2 Deverão ser fornecidos cabos de interconexão elétrica.

TERMO DE REFERÊNCIA PARA CONTRATAÇÃO DE PRODUTOS/SERVIÇOS

Atenção :

O PAGAMENTO DA NOTA FISCAL ESTÁ CONDICIONADO A ASSINATURA DA ORDEM DE COMPRAS, QUE DEVERÁ SER ENCAMINHADA JUNTAMENTE COM A NOTA FISCAL. "DE ACORDO COM A POLÍTICA DA CBV NÃO SERÃO ACEITOS BOLETOS EM NOME DE FACTORINGS OU DADOS BANCÁRIOS DE CNPJ DIFERENTE DO EMISSOR DA NOTA FISCAL."

INFORMAÇÃO SOBRE RETENÇÃO DE IMPOSTOS:

A CBV, em conformidade com as exigências impostas pela Receita Federal em sua Instrução Normativa "IN RFB 971/2009", realizará, nas notas fiscais de prestação de serviços envolvendo o uso de mão de obra, a retenção de 11% a título de INSS sobre o valor total da nota, caso não esteja especificado o valor da mão de obra e ainda a retenção de 1% sobre o valor da nota fiscal a título de retenção de imposto de renda, sendo a base de cálculo a mesma do INSS. Para notas fiscais não envolvendo serviços de mão de obra haverá a retenção de 1,5% de imposto de renda e, será recolhido ainda 4,65% (3%- COFINS + 0,65% PIS + 1% CSLL). Serão tratados individualmente os casos em que for necessário a retenção de ISS (variando entre 2% e 5% dependendo do município e atividade prestada).