BluePex®

A melhor opção para o Brasil

BluePex Firewall UTM 6.000

Especificações Técnicas Mínimas

Solução para Firewall UTM 6.000

- Gabinete para rack padrão 19 polegadas com altura máxima de 1U, com conector de console
- 16GB de memória RAM
- 10 interfaces Ethernet gigabytes
- 2 interfaces by-pass
- Processador acima de 3.40Ghz
- Fonte de alimentação full range
- Hard Disk 240 SSD
- Possibilidade de garantia de 36 meses

Fabricante

A BluePex, empresa brasileira de controle e segurança da informação é a fabricante da solução em Firewall UTM 6.000.

DESCRIÇÃO TÉCNICA

Interface gráfica administrativa, totalmente amigável e acessível por agente ou via Web.

Acesso via console de linha de comando e permitirá as seguintes configurações (para as demais configurações, deverá ser através da interface administrativa WEB):

- Configurar interface de rede;
- Configurar senha de acesso WEB;
- Reiniciar o equipamento com configuração "padrão de fábrica";
- Reiniciar o sistema;
- Parar o sistema;
- Acessar o sistema operacional do equipamento (Shell);
- Lista de atividades do Firewall, tais como conexões, gateways nos quais as conexões estão sendo roteadas e regras que estão sendo aplicadas;
- Visualizar log de filtro do Firewall;
- Reiniciar serviço de acesso WEB;
- Atualização via console;
- Habilitar acesso remoto via SSH;
- Efetuar download das dependências e de assinaturas;
- Logout para acesso via SSH;
- Funcionalidade de ping.

Primeira instalação

Utiliza auxiliador de configuração (wizard) no caso de primeira instalação do sistema.

Interface de configuração

Suporte ao idioma português do Brasil;

Configuração do produto via interface WEB ou cliente Windows de fácil compreensão.

Interfaces ou grupos de interfaces

- Grupos de Interfaces administrativas (painéis de gerenciamento) para a criação de regras que se aplicam a múltiplas interfaces sem duplicar as mesmas. Em caso de remoção de membros do grupo de interface, às respectivas regras do grupo não mais serão aplicadas àquela interface;
- Criação e uso de VLANs, mínimo 4094 VLANs 802.1Q;
- Tecnologia 3g conectado diretamente na solução firewall UTM ouNGFW, com as configurações de conexão das operadoras Brasileiras pré-configuradas.

Firewall

Características mínimas relacionadas ao sistema de Firewall:

- Statefull firewall com leitura dos 7 (sete) níveis de camada;
- Filtragem por origem e IP de destino, porta de origem do protocolo, e destino IP para o tráfego TCP e UDP;
- Capaz de limitar as conexões simultâneas com base em regras;
- Opção de gravar log do tráfego filtrando por regra;
- Possibilidade de alterar o gateway da regra de firewall para balanceamento de carga, failover, WAN múltipla;
- Agrupamento e designação de IPs, redes e portas para manter o conjunto de regras de firewall limpa e de fácil compreensão;
- Criação de regras para os mais diferenciados tipos de redes. Definir diversas interfaces e protocolos, como TCP, UDP, TCP/UDP, ICMP, ESP, AH, GRE, IGMP;
- Proteção contra ataque DoS (e/ou DDos).

Sistema de atualização de regra:

Consiga efetuar liberação de acesso a sistemas complexos como: sistemas de bancos, receita federal/sistemas do governo federal, redes sociais, entre outros com apenas 1 clique para liberação e 1 clique para salvar a regra.
Caso o acesso tenha alguma alteração como IP, porta, a BluePex Firewall UTM atualizará a regra em no máximo 24 horas a partir da notificação.

Tabela de estado:

Controle granular (ou regular) da tabela de estado (State Table) com estados e tamanhos ajustáveis, baseado nas seguintes regras:

- Limite de conexões simultâneas de cliente;
- Limite de estados por host;
- Tempo limite de estado;
- Por tipo de estado;
- Tipo do Estado com as seguintes opções: estado ativo, modular ao estado
- Limite de novas conexões por segundo;
- Synproxy - Filtrando conexões TCP para evitar excessos de SYN TCP.
- Tabela de estado: latência, normal, conexão ociosa ou legítima;

Bloqueio por país/região

- Bloqueio de conexões recebidas por determinada região;
- Bloqueio feito por país selecionando na interface de gerenciamento, onde os países estejam separados por continentes, não sendo necessário selecionar os IPs de cada país;
- Quantidade de bloqueios efetuados de cada país através de um painel gerencial (dashboard);

- Configurações extras:
  - Opção para habilitar log;
  - Configurar interface de entrada;
  - Ação a ser feita na interface de entrada (bloqueio ou rejeição);
  - Configurar interface de saída;
  - Ação a ser feita na interface de saída (bloqueio ou rejeição).

- Listas personalizadas:
  - Nome do alias e descrição
  - Ações permitidas na lista, tais como: Bloqueio de entrada, bloqueio de saída, bloqueio de entrada e saída, permitir entrada, permitir saída ou nenhuma ação;
  - Frequência de atualização a cada 1 hora.
  - Faixas de rede manualmente;
- Configuração para cada continente tal como: África, Ásia, Europa, América do Norte, Oceania, América do Sul com a lista de países e quantidade de range de IPs de cada país;
- Configuração opcional para sincronismo destas regras em caso de Cluster.

Camada 2 transparente

Permita bridge das interfaces e normalização de pacotes, evitando ambiguidades na interpretação pelo destino final do pacote, conseguindo também remontar pacotes fragmentados, protegendo sistema operacional de ataques e descartando pacotes TCP com combinações de flags inválidas.

Redirecionamento de portas

Crie regras para redirecionamento de portas, atuando como um recurso para informar ao equipamento qual o destino a ser dado aos pacotes.

NAT (Network Address Translator)

Realize a comunicação entre os hosts da rede interna e a internet, traduzindo os IPs com as seguintes características:

- Encaminhamento de portas, incluindo faixas de rede e o uso de múltiplos IPs públicos;
- 1:1NAT para IPs individuais ou sub-redes inteiras;
- NAT de saída;
- NAT de saída avançado, permitindo que seu comportamento padrão seja desativado e permitindo a criação de múltiplas flexões de regras de NAT;
- NAT Reflection - possibilitando que os serviços possam ser acessados por IP público a partir de redes internas.

IGMP Proxy

Proxy do protocolo IGMP entre segmentos de rede;

UPnP & NAT-PMP:

Permitir suporte ao protocolo UPnP e NAT-PMP, podendo configurar download e upload máximo caso necessário.

Wake on LAN

Suporte de serviço de Wake on LAN, através de suporte no hardware.

Auto Update

Suporte para atualização automática da base de seu sistema, sempre que existir alguma disponível.

Agendamentos de regras

Criação de tabela de horários para agendamento de regras;

Vincule uma regra a uma agenda definida para que as mesmas vigorem a partir de ou durante datas e horários previamente especificados;

Criação das tabelas de horários pelo administrador do sistema, bem como suas variações.

Traffic Shaper / QoS / Gerência de Banda

A solução deverá fornecer recursos de gerência de tráfego de rede;

Deverá ser possível a criação de regras dos seguintes tipos:

- Priorização de tráfego, definindo quais protocolos possui prioridade;
- Limite de tráfego por protocolo, definindo qual limite máximo de um protocolo;
- Reserva de tráfego com empréstimo em caso de não estar sendo utilizado em seu limite.
- Criação de diversas filas onde cada fila tem seu grupo de configuração;
- A configuração poderá ser definida por: interface, por fila ou layer7;

DHCP Relay

DHCP Relay encaminhe requisições para um servidor definido em outro segmento de rede.

DHCP Server

Servidor DHCP;

Atribuição de endereços IPs e configurações relacionadas aos dispositivos da rede;

DNS Forwarder para auxiliar o servidor DNS a consultar nomes na internet.

DNS Dinâmico

Uso de DNS dinâmico para que seja registrado o endereço IP público com um número de prestadores de serviços de DNS dinâmico comumente usado para conectar- se à VPNs, Web Servers e Mail Servers. Podendo ser usado conta em serviço de terceiros no mínimo usando DynDNS

LOGS

Gravação de logs das seguintes categorias:

- Log do sistema;
- Firewall;
- DHCP;
- Autenticação;
- IPSec;
- PPP;
- VPN;

Gravação de logs em servidor externo podendo configurar até 3 servidores.

Envio de informações por e-mail

Envio de informações pré-programadas referente ao status do link.

Envio de e-mail informando quando houver queda de link.

Gerência de certificados

Gerenciamento de certificados através de modo gráfico;

Criação de novos certificados através do painel web;

Revogação de certificados existentes através do painel web.

Controle de permissão de acesso

Permissão para controle para acesso às funcionalidades.

Módulo de diagnóstico

Módulo de diagnóstico com no mínimo as seguintes opções:

- Verificação da tabela ARP;
- Autenticação;
- Backup/Restore;
- Histórico de configurações;
- DNS Loup;
- Edição de arquivo;
- Voltar configuração de fábrica;
- Desligar sistema;
- Informações referentes a limites do sistema;
- Captura de pacotes;
- Tabela de roteamento;
- Tabela de estado;
- Atividades do sistema (CPU, Memória, Throughput);
- Ping;
- Traceroute.

Gerencia de Link/Banda de Internet

Load balancing no tráfego de saída para Internet com as seguintes características:

- Distribuição de carga entre duas ou mais interfaces WAN;
- O número de interfaces Wan que podem ser usadas para Load balancing, limitado à quantidade total de interfaces físicas do equipamento;
- Serviço de Load Balancer provido automaticamente à funcionalidade de Failover modo ativo – passivo;
- Balanceamento de carga de saída com múltiplas conexões WAN para fornecer balanceamento de carga e failover;
- Direcionamento do tráfego para o gateway desejado ou para o pool de balanceamento de carga em uma base de regras por firewall;
- Balanceamento inclusive entre links utilizando conexões de internet através de dispositivos USB 3G;
- Configuração do peso de cada link no momento do balanceamento para decisão de quantos pacotes deve enviar para cada link;
- Load balancing, balanceamento de entrada com as seguintes características:
- Balanceamento de carga de entrada ou failover modo ativo – passivo;
- Distribuição de carga entre vários servidores, podendo ser usado com servidores web, servidores de email e outros;

OpenNTPD

Sincronização de horário do equipamento utilizando protocolo NTP;

Possibilidade de instalar um servidor NTP dentro do Firewall, permitindo selecionar as redes no qual ele irá monitorar o serviço.

OSLR

Suporte para OLSR (Optimized Link StateRoutingProtocol).

Netflow

Protocolo Netflow versão 1, 5 ou 9 para comunicação de logs.

RIP

Protocolo RIP 1 e 2, permitindo configurar a interface e a senha.

OSPF

Protocolo OSPF caso necessário, permitindo configurar a área ou não do padrão RFC 1583.

SNMP

Protocolo SNMP.

Gráficos

Recursos inclusos:

- Sistema: Gráficos diários, semanais, mensais e anuais de:
- Memória;
- Throughput;
- Processador;

Tráfego: Gráficos diários, semanais, mensais e anuais de:

- Links;
- VPNs;
- Consumo total;

Qualidade dos links: Gráficos diários, semanais, mensais e anuais de:

- Latência;
- Perda de pacote;
- Quedas;
- Pacotes;

Possibilidade de customização de gráficos.

VPN

- Opções de VPN: IPsec, OpenVPN e o L2TP;
- Uso de VPN com outros equipamentos;
- Uso de VPN através de "client" instalado em estações de trabalho Windows;
- No caso de uso das estações de trabalho Windows, um simples "client" é apresentado;
- No caso do uso do cliente acima citado o mesmo pode ser gerado sem custo de licença e sem limites de quantidades;
- 60 algoritmos de criptografia;
- Compactação de pacotes utilizando algoritmo LZO;
- Suporte a VPN L2TP;
- Suporte a VPN PPTP Server com opção de base local ou autenticação Radius;
- Gravação de logs das conexões VPNs, em banco de dados, informando IP de origem, tempo de conexão e tráfego total.

PPPoE Server

- Suporte a PPPoE Server, com autenticação para:
  - Base local de dados de usuários;
  - RADIUS;
- Fixar IP para cada usuário;

Redundância de equipamentos

- Suporte ao funcionamento em modo Cluster e todas as licenças estão inclusas no fornecimento;
- Configuração de dois ou mais firewalls como um grupo de "failover", se uma interface falhar no primário ou ficar "off-line" completamente, o secundário se torna ativo, sem qualquer prejuízo de parada ou interrupções de atividade de operação (quantidade de usuários, conexões simultâneas, troughput, etc.) especificadas no dimensionamento;
- Capacidade de sincronização de configuração, para que as alterações de configuração no "firewall UTM ou NGFW" primário, sincronizem automaticamente com o "firewall UTM ou NGFW" secundário;
- A tabela de estado do "firewall" é replicada para todos os firewalls configurados de "failover", isso significa que as conexões existentes serão mantidas, no caso de falha, o que é importante para prevenir interrupções de rede;
- Em caso de queda de um "Firewall UTM ou NGFW", o outro assuma de modo que conexões não sejam interrompidas;

Cópia de segurança/Recuperação

Funcionalidade para fazer cópias seguras de seus dados, com no mínimo as seguintes configurações:

- Área de backup (Todos, sistema, regras de firewall, NAT, etc);
- Backups agendados;
- Backup em servidor local ou USB;

Gráficos estatísticos, monitoramento e relatórios.

Tela de Dashboard (painel de gestão) onde o administrador de redes tenha uma visão geral de todas as funcionalidades do equipamento;

O Dashboard (painel de gestão) deverá ser totalmente customizável;

Fornecer relatório e gráficos de pelo menos os seguintes itens:

- Gráficos de uso de CPU;
- Gráficos de tráfego e Throughput total da rede;
- Status dos serviços e estados do firewall;
- Serviços instalados;
- Throughput individual para cada interface:
  - Taxa de Pacotes por segundo para todas as interfaces;
  - Tempo de resposta de ping do Gateway da interface WAN;
- Bloqueio por país;
- Quantidade de dispositivos conectados em tempo real.

Fornecer relatório e gráficos de pelo menos os seguintes itens:

- Throughput em tempo real para cada interface;
- Traffic shaper a tela de status de filas QOS em tempo real de uso de fila, usando medidores atualizados;
- O Dashboard (painel de gestão) exibe medidores em tempo real do uso da CPU, memórias, swap e utilização do disco e tamanho da tabela de estado;
- Disponibiliza, em tempo real, o relatório dos sites acessados pelos usuários, mostrando informações como horário do acesso, URL acessada, ação do Proxy, categoria da URL, nome do usuário e grupo do usuário;
- Marcação dos itens liberados ou bloqueados, para facilitar a análise.

Upgrade / atualização

Atualização através da interface administrativa WEB ou através da interface Console, de maneira simples e intuitiva:

- Pacotes considerados estáveis;
- Pacotes considerados como versão BETA com objetivo de aplicação de correções rápidas para resolução de bugs críticos.

Gerenciamento Simplificado

- Módulo de gerenciamento simplificado que possua sistemas pré- configurados e atualizados diariamente comuns para liberação ou bloqueio em uma rede considerada comum, tais como: Windows Update, Java, Conectividade Social, entre outros;
- Configurações de QoS para protocolos como VOiP, entre outros;
- Configurações de Webfilter e Firewall ao mesmo tempo caso necessário;
- Portal de visitantes /Captive Portal / administração de visitantes;
- Gerenciamento de visitantes para acesso à redes sem fio para visitantes;
- Autenticação para usuários visitantes;
- Criação de regras específicas para esse grupo de visitantes;
- Criação de regras de firewall, bloqueios e controles diferentes da rede local para usuários autenticados como visitantes;

Recursos do Portal Captive:

- Máximo de conexões simultâneas;
- Tempo limite de ociosidade;
- Tempo limite rígido;
- Logon por janela de popup;
- Redirecionamento de URL após a autenticação onde os usuários podem ser redirecionados para a URL definida;
- Filtragem MAC.

Opções de Autenticação:

- Gerenciador de usuários locais;
- De autenticação RADIUS - Pode ser usado para autenticar a partir do Microsoft Active Directory e vários outros servidores RADIUS;
- Capacidades de RADIUS;
- Configuração de servidores RADIUS redundantes;
- Configuração da página inicial do Captive Portal para usar HTTP ou HTTPS;
- Upload de imagens para uso em páginas do portal.

Serviços

Os serviços e ou funcionalidades podem ser abertos conforme demanda;

É definido pelo administrador se deseja ou não instalar um serviço, a fim de otimizar recursos de hardware;

Portal de visitantes /Captive Portal / administração de visitantes

- Gerencie visitantes na rede, seja por redes sem fio ou não
- Possibilidade de autenticação e criação de regras específicas para grupo de visitantes;
- Criação de regras de firewall e bloqueios, com controle por:
  - Conexão simultânea;
  - Limite de ociosidade;
  - Limite de tempo;
  - Filtragem de MAC;
- Logon em uma janela de popup com redirecionamento para uma URL após a autenticação;
- Autenticação por usuários locais ou RADIUS;
- Permite upload de imagens;

WebFilter / Proxy

- Trabalhar com proxy transparente ou autenticado é opcional;
- É possível proxy externo;
- Exceções e bloqueios para o proxy, como: subnets permitidas, IPs que não serão filtrados, ips banidos pelo proxy e sites que terão acesso liberado pelo proxy;
- Limitar banda para hosts ou extensões como: tamanho máximo de arquivo para download, tamanho máximo para upload, limite de banda global para os hosts e limite de banda para determinadas extensões de arquivos;
- Autenticação dos usuários através de: base local, LDAP, Active Directory (AD), RADIUS, NTdomain e Single-Sign-on;
- Gerenciamento de acesso a páginas por categoria;
- Possibilidade de salvar dados em base de dados externa;

- Lista de categorias atualizadas diariamente;
- Alimentação das URL´s pertinente a cada categoria deverá ser automática e no mínimo diária;
- A base de URL´s contém mais de 50 milhões de sites catalogados;
- A base de URL´s deve conter no mínimo 48 categorias;
- Criação de categorias personalizadas sem limite de quantidades;
- Criação de lista brancas/negras como exceções;
- Redireciona as páginas bloqueadas para uma URL específica e personalizada da instituição, bem como manter a página padrão do equipamento;
- Agendamento de período em que uma regra entrará em vigor, definindo data e horário para que isto aconteça;
- Webfilter realiza escanemento contra malwares de todo o tráfego HTTP e HTTPS;
- Agendamento de backup dos logs e das configurações do webfilter;
- Módulo de diagnóstico de bloqueio ou liberação de URL por usuário, mostrando qual regra está permitindo ou bloqueando o acesso;
- Bloqueio ou liberação de múltiplos login's para acesso a internet;
- Viasualização através do painel administrativo os acessos em tempo real;
- Relatórios independentes do console de gerenciamento;
- Relatórios sem a necessidade de acessar a console de gerenciamento;
- Personalização da marca estampada no cabeçalho do relatório;
- Suíte de relatórios na mesma interface desde que com acesso restrito e de fácil utilização;

Em caso da suíte de relatórios ser em um aplicativo a parte o mesmo se transforma em multiplataforma, sendo possível ser instalado em Windows ou Linux ou MAC, com funcionamento externo ao produto;

A solução gera relatórios de navegação referentes a usuários, domínios ou relatórios resumidos com pelo menos as seguintes características:

- Acessos por Usuários Analíticos;
- Consumo de Link por Usuário;
- Acessos por IP Analítico;
- Consumo de Link por IP;
- Atividades por Usuários;
- Atividades por IP;
- Sites mais acessados Analíticos;
- Consumo de Link por Site e Sites por usuários;
- Acessos por categoria e Consumo de link por categoria;
- Quantidade de acessos por IP sintético ou analítico;
- Duração da conexão de VPN por usuário;
- Consumo de banda por usuário de VPN;
- Duração da conexão de VPN por IP;
- Consumo de banda por IP de VPN;
- Relatório resumido que informa o consumo total de banda utilizado pelo Proxy;
- Todos os relatórios anteriores podem ser gerados pelo menos nos seguintes formatos: PDF, CVS, HTML;

Suporte a protocolo BGP

Suporte ao protocolo BPG segundo RFC 4271;

Em caso de "failover" configurado através do protocolo BGP, o sistema mantem conexões ativas caso ocorra queda em algum link e o outro link esteja em perfeito funcionamento e possua tamanho de banda compatível;

As conexões VoIP, banco de dados e ERP's, permanecem ativas mesmo em caso de queda de um dos links.

Uso de Rede

Visualize dados de uso da rede de modo interativo, com suporte também a NetFlow/sFlow em uma interface baseada em HTML permitindo criar aplicações de monitoramento ntop-centric e RRD para estatísticas de tráfego.

IPS

Sistema de detecção e prevenção de intrusão com capacidade de inspecionar o “payload” do pacote, fazendo o registro dos pacotes, além de detectar as invasões. Capaz de detectar quando um ataque está sendo realizado e, baseado nas características do ataque, alterar ou remodelar sua configuração de acordo com as necessidades, além de permitir a configuração de avisos ao administrador do ambiente sobre o ataque;

A solução de IDS/IPS permite configurar alertas;

Registro através de um cadastro denominado Whitelist as redes ou IPs dos computadores que o IDS/PS não aplicará as suas regras de bloqueio.

Antivírus de navegação

HTTP Antivírus para scanner de vírus para todo download efetuado.

Licenças para o antivírus.

.

BluePex®

bluepex.com falecom@bluepex.com 0800 771 71 72

Parceiros e Associados:

UNICAMP virustotal Softex vb100 VIRUS virusbtn.com ABIMDE ABES SOFTWARE Microsoft Partner