comportamento das aplicações) e categorias de aplicações;
5.6.2.63. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
5.6.2.64. Firewall deve ser capaz de aplicar a inspeção UTM (Application Control e Webfiltering no mínimo) diretamente às políticas de segurança versus via perfis;
5.6.2.65. Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente às políticas de firewall;
5.6.2.66. Ele deve suportar a automação de situações como detecção de equipamentos comprometidos, status do sistema, alterações de configuração, eventos específicos e aplicar uma ação que pode ser notificação, bloqueio de um computador, execução de scripts ou funções em nuvem pública.
5.6.2.67. Deve suportar o padrão de indústria 'syslog' protocol para armanazemento usando o formato Common Event Format (CEF);
5.6.2.68. Deve haver uma maneira de assegurar que o armazenamento dos logs em tempo real não superam a velocidade de upload;
5.6.2.69. Deve suportar o protocolo padrão da indústria VXLAN;
5.6.2.70. Deve suportar objetos de endereço IPv4 e IPv6, consolidados na mesma regra/política de firewall
5.6.2.71. Deve possuir base com objetos de endereço IP, de serviços da internet como Google e Office 365, atualizados dinamicamente pela solução
5.6.2.72. A solução deve oferecer suporte à integração nativa com a solução de sandbox, proteção de email, cache e firewall de aplicativos da Web.
5.6.2.73. Controle de Aplicações
5.6.2.74. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
5.6.2.75. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
5.6.2.76. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms -rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
5.6.2.77. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
5.6.2.78. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
5.6.2.79. Identificar o uso de táticas evasivas via comunicações criptografadas;
5.6.2.80. Atualizar a base de assinaturas de aplicações automaticamente;
5.6.2.81. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;
5.6.2.82. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
5.6.2.83. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
5.6.2.84. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
5.6.2.85. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
5.6.2.86. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
5.6.2.87. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;
5.6.2.88. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
5.6.2.89. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);
5.6.2.90. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;
5.6.2.91. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
5.6.2.92. Deve ser possível configurar Application Override permitindo selecionar aplicações individualmente;
5.6.2.93. Prevenção de Ameaças
5.6.2.94. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;
5.6.2.95. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
5.6.2.96. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;
5.6.2.97. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
5.6.2.98. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
5.6.2.99. Deve permitir o bloqueio de vulnerabilidades;
5.6.2.100. Deve incluir proteção contra ataques de negação de serviços;
5.6.2.101. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise de decodificação de protocolo;
5.6.2.102. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise para detecção de anomalias de protocolo;
5.6.2.103. Deverá possuir o seguinte mecanismos de inspeção de IPS: IP Defragmentation;
5.6.2.104. Deverá possuir o seguinte mecanismos de inspeção de IPS: Remontagem de pacotes de TCP;
5.6.2.105. Deverá possuir o seguinte mecanismos de inspeção de IPS: Bloqueio de pacotes malformados;
5.6.2.106. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
5.6.2.107. Detectar e bloquear a origem de portscans;
5.6.2.108. Bloquear ataques efetuados por worms conhecidos;
5.6.2.109. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
5.6.2.110. Possuir assinaturas para bloqueio de ataques de buffer overflow;
5.6.2.111. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
5.6.2.112. Identificar e bloquear comunicação com botnets;
5.6.2.113. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
5.6.2.114. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
5.6.2.115. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
5.6.2.116. Os eventos devem identificar o país de onde partiu a ameaça;
5.6.2.117. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
5.6.2.118. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
5.6.2.119. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;
5.6.2.120. Suportar e estar licenciado com proteção contra ataques de dia zero por meio de integração com solução de Sandbox em nuvem, do mesmo fabricante;
5.6.2.121. Filtro de URL
5.6.2.122. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
5.6.2.123. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local, em modo de proxy transparente e explícito;
5.6.2.124. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
5.6.2.125. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
5.6.2.126. Possuir pelo menos 60 categorias de URLs;
5.6.2.127. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
5.6.2.128. Permitir a customização de página de bloqueio;Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);
5.6.2.129. Além do Explicit Web Proxy, suportar proxy Web transparente;
5.6.2.130. Identificação de Usuários
5.6.2.131. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;
5.6.2.132. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;
5.6.2.133. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à, utilização de sistemas virtuais, segmentos de rede, etc;
5.6.2.134. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;
5.6.2.135. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários;
5.6.2.136. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);