# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRODUCTION</td>
<td>5</td>
</tr>
<tr>
<td>TECHNICAL ADVANTAGES</td>
<td>6</td>
</tr>
<tr>
<td>MARKET FACTORS</td>
<td>8</td>
</tr>
<tr>
<td>CUSTOMER GROUPS</td>
<td>8</td>
</tr>
<tr>
<td>VALUE-ADDED SERVICES</td>
<td>8</td>
</tr>
<tr>
<td>SERVICE PROVIDER BENEFITS</td>
<td>9</td>
</tr>
<tr>
<td>PRODUCT HIGHLIGHTS</td>
<td>11</td>
</tr>
<tr>
<td>AUDITING AND REPORTING</td>
<td>12</td>
</tr>
<tr>
<td>ACCURACY AND PERFORMANCE</td>
<td>12</td>
</tr>
<tr>
<td>APPLICATION PROTOCOLS</td>
<td>13</td>
</tr>
<tr>
<td>CONTENT CATEGORIES</td>
<td>14</td>
</tr>
<tr>
<td>ADVANCED PACKET FILTERING</td>
<td>15</td>
</tr>
<tr>
<td>USER TO INTEGRATION LEVEL</td>
<td>15</td>
</tr>
<tr>
<td>DENY PAGE BRANDING AND MONETIZATION</td>
<td>16</td>
</tr>
<tr>
<td>INTEGRATION TO DISTRIBUTION LEVEL</td>
<td>16</td>
</tr>
<tr>
<td>DISTRIBUTION TO CATEGORIZATION LEVEL</td>
<td>17</td>
</tr>
<tr>
<td>PROACTIVE WEB SECURITY</td>
<td>19</td>
</tr>
<tr>
<td>DENY PAGE BRANDING AND MONETIZATION</td>
<td>20</td>
</tr>
<tr>
<td>DIRECTORY SERVICE SYNCHRONIZATION</td>
<td>21</td>
</tr>
<tr>
<td>NETWORK UBIQUIETY</td>
<td>22</td>
</tr>
<tr>
<td>CONSIDERATIONS FOR NETWORK DEPLOYMENT</td>
<td>23</td>
</tr>
<tr>
<td>NETWORK SERVICE COMPONENTS</td>
<td>24</td>
</tr>
<tr>
<td>INTERCEPTION DEVICE</td>
<td>24</td>
</tr>
<tr>
<td>POLICY SERVER</td>
<td>24</td>
</tr>
<tr>
<td>WEB SERVER</td>
<td>25</td>
</tr>
<tr>
<td>REPORTER</td>
<td>27</td>
</tr>
<tr>
<td>3RD PARTY INTERCEPTORS</td>
<td>27</td>
</tr>
<tr>
<td>DETERMINING PHYSICAL NETWORK LOCATION</td>
<td>28</td>
</tr>
<tr>
<td>DEPLOYMENT EXAMPLES</td>
<td>30</td>
</tr>
<tr>
<td>SERVICE PROVIDER CORE NETWORK</td>
<td>30</td>
</tr>
<tr>
<td>HIGH DEMAND NETWORK</td>
<td>31</td>
</tr>
<tr>
<td>ESTIMATING PLATFORM REQUIREMENTS</td>
<td>32</td>
</tr>
<tr>
<td>SUPPORT AND MAINTENANCE</td>
<td>33</td>
</tr>
<tr>
<td>BASIC WARRANTY SUPPORT</td>
<td>33</td>
</tr>
<tr>
<td>ADVANCED SERVER REPLACEMENT</td>
<td>33</td>
</tr>
<tr>
<td>ADVANCED PARTS REPLACEMENT</td>
<td>34</td>
</tr>
<tr>
<td>ADVANCED PARTS REPLACEMENT WITH ON-SITE TECHNICIAN</td>
<td>34</td>
</tr>
<tr>
<td>ANYTIME ON-SITE</td>
<td>34</td>
</tr>
<tr>
<td>ANYTIME ON-SITE WITH ADVANCED TROUBLESHOOTING</td>
<td>34</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>TECHNICAL SUPPORT SERVICES</td>
<td>35</td>
</tr>
<tr>
<td>SPECIFICATIONS</td>
<td>36</td>
</tr>
<tr>
<td>RECOMMENDED CARRIER GRADE PLATFORM</td>
<td>36</td>
</tr>
<tr>
<td>PACKET FILTERING AND WEB SECURITY</td>
<td>36</td>
</tr>
<tr>
<td>CONCLUSION</td>
<td>37</td>
</tr>
</tbody>
</table>
INTRODUCTION

Netsweeper specializes in advanced packet filtering and proactive web security managed services to provide the industry’s most sophisticated dynamic packet analysis, content categorization, policy management, and Internet protection services.

Efficient and secure management of Internet content and traffic pattern analysis has become more strategic as cable, wireless, fixed-line, satellite and virtual network operator service providers employ next generation services, content, and evolving addressing systems like Uniform Resource Identifiers (URIs).

Traditional content filtering solutions are stretched way beyond their limits attempting to deal with service provider billing, provisioning and advanced data network and content licensing environments. The remarkable increase of mobile web enabled devices, highly dynamic sites, subscriber-initiated content, and growing web threats like drive-by downloads make it impossible for service providers to provision and bill subscribers, and filter packet data networks meaningfully using static based unintelligent content filtering solutions.

Netsweeper offers proven technology to implement scalable, bi-directional packet filtering and web security services that are fully compatible with service provider provisioning, billing and subscriber authentication strategies.

A breakthrough for packet filtering and web security, Netsweeper provides unmatched carrier grade value-added services for cable, wireless, fixed-line, satellite and virtual network operator service providers.
TECHNICAL ADVANTAGES

Netsweeper packet filtering and web security services use Artificial Intelligence (AI) technology to dynamically traverse content and make real-time decisions based upon algorithms developed from over a decade of collected content and trend analysis. Dynamic categorization and policy management services automatically standardize data formats and fields from content and country-specific URIs into a common, normalized format for more than 200 countries and 90 application protocols and content categories.

The AI technology is the industry’s most comprehensive real-time classification of unclassified URLs based on dynamic analysis and categorization of content, providing unmatched packet filtering, anti-virus and anti-malware web protection, application control, and Internet usage policy management and reporting.

At over 200,000 requests per second, a single low-end server platform running the Netsweeper system providing packet filtering, web security and policy management services is able to respond to URI requests in less than three milliseconds, while the dynamic analysis and categorization process simultaneously scans, analyzes and classifies embedded links for the most current review of an entire website’s safety and content. This instantaneous analysis and categorization provides immediate insight into threats, blocking inappropriate and harmful content at the zero hour, well before our customers are exposed to them.

Unlike static URL filtering lists, Netsweeper services allow websites to move from harmful to safe based on changes in content. So a URL or website that has been compromised and assigned a harmful or inappropriate rating can be redeemed after all traces of malware or inappropriate content have been removed.

Known and newly discovered URLs are dynamically analyzed, updated and categorized in globally distributed databases that are instantaneously made available to all customers worldwide. The automated content categorization includes built-in real-time feedback to ensure complete accuracy.

With over 3 billion active URLs categorized and growing by over 10 million per day, Netsweeper’s carrier grade packet filtering, web security, policy management, and categorization services lead the industry.

The distributed architecture of Netsweeper service platforms enables flexible deployment across multiple locations to accommodate performance management and disaster recovery strategies. All service platforms are also available on highly resilient and available Network Equipment Building Systems (NEBS) Level 3 compliant communication systems platforms for added fault tolerance.

Support for all major directory services (RADIUS, LDAP, Active Directory, eDirectory) enables complete integration with all types of subscriber authentication and content licensing strategies.
Policy management services comply with all international government, social, cultural, legal, educational, security and corporate policies. Complete regulatory compliance is possible because categories and filtering policies are fully customizable, whereby service providers are able to modify and expand packet filtering categories and policies to meet evolving requirements.

Service providers can confidently deploy Netsweeper carrier grade services to increase revenue and exceed requirements for intelligent packet filtering, web security, and dynamic categorization and policy management value-added applications.
MARKET FACTORS

With the advent of 3G, 4G, WiMax and other next-generation networks, subscriber access to content is growing exponentially. Additionally, the convenience of Internet access encourages subscribers to access a larger amount and array of content.

While this enables new applications and revenue streams for service providers, it also creates new concerns relating to content licensing, security, productivity, availability and the appropriateness of content for different groups of subscribers.

It's become increasingly strategic for service providers to work together with businesses, governments, law enforcement, families, schools and child safety organizations to ensure that each group understands their responsibilities.

Customer Groups

The following customer groups have specific requirements to manage Internet access, filter packets, and analyze traffic patterns and trends to filter inappropriate content, enhance web security, increase productivity, and protect against liability for legal, cultural, religious, ethical, or other personal or social reasons.

- Consumers (Individual Subscribers, Parents and Caregivers)
- Religious and Library Institutions
- SMB, Enterprise and Global Corporations
- K-12, Private, Public, College, University, and Other Educational Institutions
- National and International Defense Forces and Intelligence Agencies
- Local, State, Provincial, National and International Government and Law Enforcement

Value-added Services

Service providers can offer advanced packet filtering and proactive web security services to specific customer groups to differentiate service, or offer them as value-added services for increases revenue as a part of supplementary or bundled service offerings.

For example, service providers might offer advanced packet filtering and proactive web security services to consumers as a part of their Internet service, while other customer groups might be billed for the services separately or offered the services together as a part of negotiated or advertised service agreements.

As another example, service providers might offer a basic filtering service to shield underage users or businesses from inappropriate content or illegal
content such as Child Pornography, and bill for value-added filtering services such as applying more policies at different times of day or allowing for a more granular and nuanced choice of filtering categories.

The following value-added services are enabled by Netsweeper advanced packet filtering and proactive web security.

- Security – Real-time protection from emerging web threats – 0 day outbreaks
- Policy Compliance and Parental Control – Prevent browsing of inappropriate content and applications
- Productivity – Block, monitor and report on access to specific content and applications
- Bandwidth Regulation – Manage content that consumes bandwidth (E.g. movies, music)
- Advertising and Sales – Enable new online advertising and sales situations
- Content-based Billing – Control access to content and applications based on subscription services

Service Provider Benefits

Advanced packet filtering, web security and policy management value-added services can strategically improve the following service provider programs.

- ARPU – Flexible value-added packet filtering and web security services with tiered pricing supplement recurring revenue streams with each type of customer.
- Customer Loyalty – Differentiated packet filtering and web security services satisfy each customer’s requirements providing best-in-class customer centric services that are associated with excellence.
- Service Provider Image – Ethical management of access to unacceptable types of content, and protection of customers from harmful malware and other potential dangers of the Internet.
- Advertising Revenue – Monetization of deny page content to enhance high-value advertising revenue sharing and joint marketing partnerships with OEMs, retailers, and other service provider partners. Produce highly targeted advertising models for content owners, licensors and brand managers to reach specific subscribers directly through focused demographics and other selective marketing initiatives.
- Targeted e-Commerce Sales – Strategic marketing of content specific e-commerce sales related products and services to subscribers. As with highly targeted online advertising, secure profitable revenue sharing and referral sales relationships with a wide range of online retailers as well as with OEM and other service provider partners.
- Service Offering – Web security that prevents access to harmful or unauthorized Internet content enhances infrastructure performance and content deployment strategies to optimize infrastructure and bandwidth utilization.

- Content Access Management – Controlled access to licensed and subscription-based content. Enforce content access and licensing restrictions using subscriber authentication and packet filter blocking of proxy anonymizer services.

- Regulatory Compliance – Compliance with European Union, North American, and other international and child safety regulations. For example, educational institutions in the United Kingdom, Germany, the United States, and other countries already have policies to help prevent underage subscribers from viewing inappropriate content.
PRODUCT HIGHLIGHTS

- Delegated Management – Enables delegated organizational and group control over subscribers for which they are responsible. All policies can be reviewed using central web-based administration to ensure that organizations and groups are in-line with Internet usage policies. Distribution of the administration reduces service provider responsibilities by empowering customers and subscribers to create and enforce Internet usage policies.

- Secure (SSL) Web-Based Administration - Provides the flexibility to administer packet filtering and web security policies from a web browser anytime and anywhere.

- Network Mobility – Highly configurable and enforceable Internet usage policies and web security for mobile devices. Enables the industry’s only fully integrated mobile device packet filtering solution for integrated policy management and reporting for mobile devices.

- Proactive Web Security – Detects known and zero-hour or unknown web-based virus and malware threats, providing the most effective protection against malicious content by correlating a combination of current traffic and request trends, multiple detection technologies, automated machine-learning heuristics, and the industry’s largest data set of web content.

- Global, Group and Individual Subscriber Internet Usage Policies – Enforces multiple policies for any number of groups and subscribers. Moving subscribers and groups to other Internet usage policies, or creating new Internet usage policies, is quick and simple. Provides immediate compliance with corporate, educational, and government policies, while allowing unregulated or less restricted access for other groups and subscribers.

- Blacklist/White list Management – Organizations and groups can create and import custom lists of acceptable or unacceptable websites. A website can be included in a White list to allow access or a Blacklist to deny access if authorized organizations or groups wish to override the categorization of the website.

- Scheduled Filtering and Filtering Overrides – Groups, organizations and individual subscribers can manage time of day settings for the filtering and adjust the filtering policies as required. Additionally, groups, organizations and individual subscribers can be set to override the filter (although silent tracking can still be performed).

- Master Deny Lists – Industry’s largest collection of categorized website information which is used when setting up policies. These lists include the Internet Watch Foundation, Phishing lists, etc.
Auditing and Reporting

- Comprehensive Reporting – Groups, organizations and individual subscribers have the ability to track, view and report on Internet activities. Reports can provide information by directory service user id, group and IP Address, and can be viewed in real-time and by date and time.
- Consolidated Reports – Simplifies Internet usage reporting for incident handling and forensics
- Silent Tracking – Instinctively survey, examine, and understand granular network packet content and application protocol usage across network infrastructure, and establish policies based on information. Service providers can better understand which types of subscribers are accessing which types of websites and applications.
- Flexible Report Delivery – In addition to HTML, CSV, XML or PDF output, report output can be provided in popular export formats and automatically delivered to multiple email accounts.
- Validation – Reporting and logging capabilities can also be used to validate the use of educational, corporate of government content or application protocols implemented for use by specific groups. Using the web interface, organizations can easily create a custom category for specific application protocols and content. Activity is reported by subscriber, device, or group for the specified application protocols and content categories.
- Performance – Reporting services are extremely comprehensive, and were specifically designed to efficiently handle extremely large log files. Size of the log files are automatically managed based on available disk space. Log files can be backed up for archival purposes or can be stored on large SAN or NAS storage systems.

Accuracy and Performance

- Industry’s Largest and Most Current URI Database – Over 3 billion categorized URIs and receives requests for approximately 10 million new URIs each day.
- On-Demand Categorization – When new URIs are encountered, content on the page is automatically categorized in real-time. With content constantly being added to the Internet, only on-demand categorization can truly enforce Internet access management policies.
- Proxy Anonymizers – On-demand real-time categorization ensures that these proxy sites are unavailable for any attempts to bypass Internet access management policies.
• Quarantine – Block all Internet access to users who repeatedly try to bypass filtering or access URIs that have been infected with a virus preventing the spread to other systems.

• Scalability – The service architecture is designed to scale from a small deployment of a few workstations to large in-the-cloud bi-directional core deployment with Tier 1 carriers and service providers filtering packet data networks for millions of subscribers.

• Managed Services – Packet filtering and web security services can be private labelled or branded for service providers and their customers.

• Scalability – Packet filtering and web security service platforms can be virtualized and/or distributed to scale to any network throughput. As the number of subscribers or volume increases, service providers can sustain performance by simply adding additional low cost platforms. Load-balancing techniques distribute the traffic between platforms for optimal performance.

• Availability – Service platforms can be deployed in a redundant configuration, either within a single data center or distributed over multiple data centers. Failover prevents transactions from being interrupted in the event of a platform failure. NEBS Level 3 compliant platforms are also available for added fault tolerance.

• CIPA compliant – Netsweeper complies with the requirements outlined in the Children’s Internet Protection Act signed to law in the United States in 2000. Schools and libraries seeking E-Rate discounts must adhere to CIPA regulations in order to fully qualify for these discounts. According to Wikipedia, “CIPA requires schools and libraries using E-Rate discounts to operate "a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are obscene, child pornography, or harmful to minors..."

• Becta accreditation – Netsweeper was the first Internet content filtering solution in the market to adhere to the standards but forth by the British Educational Communications and Technology Agency. Becta is a government body whose purpose is to influence the use of technology in learning. As part of its mission, Becta will research and test technology tools of various sorts and then put forth their recommendations to the education community.

**Application Protocols**

• Instant Messaging – ICQ/AIM, IRC, Jabber, MSN File Transfers, Microsoft Messenger, MySpaceIM, Paltalk, QQ, Yahoo Messenger

• File Transfer – AppleJuice, Ares, BearShare, BitTorrent, Direct Connect, Gnutella, Kazaa, LimeWire, Mute, Napster, OpenFT, Soulseek, eDonkey
Advanced Packet Filtering and Proactive Web Security

- E-mail – IMAP Incoming Mail, Outgoing Mail (SMTP), POP3 Incoming Mail
- VoIP – H.323, Roger Wilco, SIP - Internet telephony, Skype, Ventrilo
- Streaming Media – RTSP, Real Player, Winamp, Windows Media Player, iTunes
- Miscellaneous – JAP, News Groups, PC Anywhere, RDP, SOCKS, SSL/TLS, SSH

Content Categories

- Adult – Adult Image, Alcohol, Alternative, Criminal Skills, Extreme, Gambling, Hate Speech, Lifestyles, Match Making, Occult, Pornography, Profanity, Substance Abuse, Weapons
- Entertainment – Arts & Culture, Educational Games, Entertainment, Games, Humor, Sports
- Information – General News, Journals and Blogs, Political, Portals, Religion, Self Help, Sex Education, Social Networking, Technology, Travel
- Security – Adware, Directory, Host is an IP, Intranet Servers, Malformed URL, Phishing, Proxy Anonymizer, Viruses and Malware
- Miscellaneous – Investing, Job Search, Sales, Search Engine, Web Chat, Web E-mail
- Advanced – General, Images, Network Timeout, Network Timeout, Network Unavailable, New URL, No Text Redirector Page, Safe Search, Search Keywords
- Custom Categories – e.g. Extreme Sites for Racism
ADVANCED PACKET FILTERING

The advanced packet filtering service offers service providers proven technology with immense flexibility and options to implement scalable bi-directional filtering and analysis for dynamic content analysis and categorization. Bi-directional filtering provides packet analysis, web security and detailed content and protocol statistical reporting for outbound Internet requests by subscribers and inbound Internet requests to service provider or hosted Internet services.

To solve traditional limitations with purely list-based filters, Netsweeper developed a dynamic “cloud computing” approach to packet filtering for both protocol and content analysis and categorization over 10 years ago. This distributed “in the cloud” packet filtering approach processes billions of transactions daily overcoming storage limitations brought about by the vast size of the Internet and diverse browsing habits of users.

Packet filtering services use a combination of globally distributed databases of categorized URIs and Policy Servers to analyze, categorize, cache and control access to only URIs accessed by resident users. The availability and speed of the solution is a key benefit, as it means less than 10 milliseconds of latency even in the most heavily used networks.

If a user visits a URI not cached in a local Policy Server database, the URI is requested from a central databases or Category Name Server (CNS). The CNS provides information about the requested URI to the Policy Server, which caches the information to be ready if the request is made again. This ensures that Policy Servers only cache up-to-date and relevant URIs.

If a CNS does not have the requested URI in its database, a categorization engine scans the URI on demand, categorizes it, and provides information about the requested URI to the Policy Server.

Both known and unknown URIs are sent to categorization engines to determine most current content and category. At the same time all linked URIs are checked for associations and categorized to maintain the most up-to-date information about each URI. All associated updates and new URIs are simultaneously added to the requesting CNS and Policy Server caches.

User to Integration Level

When a user makes a request for a specific URI, the packet filter intercepts the request and asks the Policy Server for a ruling - whether to allow or deny the connection.

The Policy Server must first determine the outgoing request: Is it a protocol request or an HTTP request? For non-HTTP requests (such as VoIP, messaging or file sharing), the Policy Server is always able to make the categorization itself based on the policy. If it is an HTTP request, the Policy Server checks its own cache for the URI, and after the URI is identified, the Policy Server categorizes the request.
After the Policy Server categorizes the request it looks up the group policy associated with the user who made the request.

Policies can be defined as blanket policies covering all users and groups. It is also possible to define different policies for different times of the day.

If the specific policy allows the outgoing request, the policy service is told to process the request.

If the specific policy does not allow the category of the outgoing request, the policy service returns a deny page or returns a HTTP error response code (such as 403, 404, 500) to the user that indicates the reason the request was not fulfilled.

**Deny Page Branding and Monetization**

Requests for content that are redirected to deny pages warn users that the requested content was not authorized.

The packet filter service offers service providers immense flexibility and options to brand and monetize deny pages. Implemented correctly, branding and monetization of deny pages can provide tremendous advertising and revenue generation opportunities.

**Integration to Distribution Level**

The Policy Server is designed to cache only requested URIs to eliminate resource-intensive updates and maximize response time and accuracy of cached URIs. If a Policy Server is not able to locally categorize an HTTP request, it sends the URI to a Category Name Server (CNS) requesting a category ruling. Like the Policy Server, the CNS maintains a local cache of requested URIs and first looks here to assign a category to the URI.

If the URI is in the CNS cache, the CNS returns the category for the URI to the Policy Server.

If the CNS does not have the requested URI’s category in its cache, the CNS sends the URI to the Master Category Name Server (MCNS) requesting a category ruling for the URI, and returns a new URI category to the policy server immediately. The MCNS updates massive centralized database stores with global URI categorizations.

Policy Servers are either deployed on platforms within the service provider core network or on the edge or perimeter of customer networks.

Category Name Servers are normally hosted by Netsweeper in the service provider’s network. A CNS can also be dedicated to a particular customer or group of customers and may contain its own local URL list – for example, static allow/deny lists.

On a new URI response, the Policy Server proceeds to process the initial request from the packet filtering service using “New URL” as the category. Without a category for the URI, the Policy Server looks up the ruling and responds to the
packet filtering service to temporarily allow or deny. The Policy Server stores the URI in its cache with the category of new URL for a period of 60 seconds. If the URI is requested the URI will then be updated with an updated category and a longer expiry date.

**Distribution to Categorization Level**

Continuing upstream, if the MCNS does not have the URI in its own cache, it returns a new URL to the CNS server, which results in a New URL being stored in the CNS cache for up to 60 seconds.

The MCNS then requests a category ruling for the URI from the categorization system which downloads and analyzes the URI and assigns a category.

The categorization engine is made up of a number of processes running thousands of threads; each processing URI categorization requests. The categorization engine reviews the URI content and, within microseconds, assigns a category to the requested URI.

When the categorization engine receives a request, it retrieves the URI, parses the data, reports any found embedded links to the MCNS for their own category ruling, and proceeds to determine a category for the original URI request. Once it determines a category for the URI, it passes the data to the MCNS which updates the categorization database. The categorization database uses multiple distributed SQL database servers to balance the URI request load to support disaster recovery and business continuity plans.

New URL is one of several special system categories. The administrator can set the filtering policy to allow or deny URIs with the New URL category (or other system categories) to tailor the overall response.

For New URL categorizations, the servers (Policy, CNS and MCNS) know to request a refresh of the category for the URI (since the categorization engine will have categorized the URI at this point and updated the categorization database).

The entire categorization process — from initial request for a URI never seen by the system before (worldwide) to categorization engine result and storage in the database — takes as little as one second and at most five seconds, depending on the global location of the user and the speed of connection to the requested URI.

Users and administrators are able to request a human review of URIs—either to add a URI to a category, remove a URI from a category, or add a URI to multiple categories. All sites reviewed manually are immediately updated in the categorization database and are made available to CNS servers.
The following diagram depicts a simplified version of what happens when users make outgoing URL requests through a Netsweeper packet filtering solution.
PROACTIVE WEB SECURITY

Service providers are adopting more comprehensive proactive anti-virus and anti-malware web security services as part of the need to improve network security strategies and protect network infrastructure and subscriber web enabled devices from malicious threats.

Netsweeper’s proactive web security service offers service providers proven technology with immense flexibility and options to implement scalable bi-directional filtering and analysis for signature-base and dynamic viruses, malware and other script-based threats.

The web security service operates as a part of the categorization process to immediately detect known and zero-hour or unknown virus and malware threats. The service provides the most effective protection against new and known malicious content by correlating a combination of current traffic and request trends, multiple detection technologies, automated machine-learning heuristics, and the industry’s largest data set of web content.

More specifically, the web security service protection includes:

- Signature-based anti-virus and anti-malware that provides security against previously identified viruses with immediate updates and responses to new threats
- Dynamic anti-virus and anti-malware that provides string scanning and advanced heuristic technology designed to stop unknown web-based viruses and spyware
- Web browser attack protection that provides malicious script scanning to stop script-based threats that look inside application sessions to determine the intent of active content passed between the server and the browser

Signature-based scanning detects known malware residing on both reputable and uncategorized websites. As is expected in a signature based solution, Netsweeper’s solution uses multiple anti-malware scan engines which cover all known spyware and viruses with regular hourly updates, and immediate updates for outbreaks. All requested URIs are automatically scanned and categorized, even known URIs are scanned to ensure current legitimacy.

Heuristic engines use non-signature detection techniques and are based upon Artificial Intelligence (AI) technologies used to traverse the content and make decisions based upon thousands of inputs trained from over a decade of collected information and trends.

Using signature-based scan engines, heuristic detection engines and correlating real-time trends of requests provides an unparalleled advantage in providing zero-hour protection. The categorization process filters millions of requests a second from around the world in multiple languages, multiple sectors and multiple areas of information. Over 10 million requests per day are for new uncategorized URLs which were never been seen before. With over a decade in
operation and more than 3 billion active URIs categorized, Netsweeper has an unrivalled view of demographically accurate web history and usage.

The web security service also immediately sees outbreaks of malicious code through the trend of requests, independently of the initial vector of propagation. If a new SPAM message or IM chat traverses the Internet with an image, document or link sending subscribers to a web-based threat, the traditional approach of scanning the endpoint has shown vulnerabilities with lagging signature updates, lack of worldwide visibility and little trend information. In this case, a correlation of the immediate rush of requests, the history and a real-time content analysis allow the heuristic engines to block the malicious content in real-time, before any subscribers become infected.

**Deny Page Branding and Monetization**

Requests for content that contain viruses, malware, browser attacks or other script base threats are redirected to deny pages that warn subscribers that the requested content contains a harmful virus, malware or malicious threat giving the subscriber the option to click through to the infected web page.

The web security service offers service providers immense flexibility and options to brand and monetize deny pages. Implemented correctly, branding and monetization of deny pages can provide tremendous advertising and revenue generation opportunities.
DIRECTORY SERVICE SYNCHRONIZATION

Netsweeper supports automatic directory service synchronization with Active Directory, eDirectory, LDAP and RADIUS. Service providers can easily integrate packet filtering and web security services with current identity management strategies, and can also offer their education, corporate and government customers seamless integration with native identity management and directory service infrastructures.

Netsweeper directory service synchronization imports users or subscribers from customer directory services to the Policy Server. The existing structures of the groups will also be recreated on the Policy Server.

The directory service synchronization will continue to run in the background to automatically synchronize changes with customer directory services, thus automatically updating the Policy Server.

The following diagram illustrates an example of Microsoft Domain Controller Active Directory synchronization.
NETWORK UBIIQUITY

Using normal subscriber authentication techniques, packet filtering and web security services extend beyond the network perimeter to provide integrated solutions specifically designed for cable and wireless devices. This enables ubiquitous packet filtering and web security services globally throughout the network and to the mobile Internet edge on any authenticated wireless or WLAN netbook, laptop or mobile device – all without installing any software on the mobile device.

The open architecture of the Policy Server supports seamless integration with cable, wireless, and satellite broadband authentication, authorization, and accounting (AAA), and Operational Support Systems (OSS) provisioning and billing services (BSS) to ensure smooth deployment for service providers.

Support for all major directory services (RADIUS, LDAP, Active Directory, eDirectory) enables integration with virtually all types of identity management and subscriber authentication.

For example, packet filtering and web security service authentication extends to mobile wireless devices using a RADIUS proxy for AAA and OSS provisioning and billing. When subscribers request content on a mobile wireless device, the IP address can be mapped to either a username or a Mobile Subscriber ISDN (MSISDN) that can be used to authenticate the subscriber using RADIUS.

Once a subscriber is authenticated, the Policy Server can then be used to determine if packet filtering and web security services are enabled. If the profile indicates that packet filtering and web security is not enabled for the subscriber, no further involvement is needed from the Policy Server. If packet filtering and web security services are enabled for the subscriber, appropriate Policy Server services are applied to the subscriber.

Additionally using this same technique, packet filtering and web security service authentication extends to cable modem devices using a RADIUS or LDAP proxy for AAA and OSS provisioning and billing. When subscribers request content on a cable modem device, the cable modem MAC address can be mapped to either a username or account that can be used to authenticate the subscriber using RADIUS or LDAP.

Unauthenticated netbook and laptop mobile device subscribers can even be protected outside a network perimeter by simply installing a Layered Service Provider shim on the client device to identify the subscriber and intercept and modify inbound and outbound TCP/IP traffic.
CONSIDERATIONS FOR NETWORK DEPLOYMENT

Netsweeper service platforms are made up of separate service components that can be deployed together on a single Intel based platform or independently and load balanced across multiple Intel based platforms depending on specific network infrastructure and performance requirements.

Service providers have complete flexibility to size and distribute service platforms to optimize network scalability and availability across a wide variety of network infrastructure environments ranging from implementations on small private networks to implementations on extremely large core carrier-grade networks.

Service providers and their customers can choose to deploy either Netsweeper service platform appliances or their own preferred vendor Intel based platform.

The two main service components are the packet filter Interception Device and the Policy Server. Other components are the Database, Web Server and Reporter.

- **Interception Device** – The service (or other 3rd party interceptors) that intercepts traffic and ultimately carries out allow or deny rulings.

- **Policy Server** – The service that matches web requests with category assignments and makes allow or deny rulings based on the user’s Policy.

- **Database** – The service that stores the system and Policy Server configuration settings.

- **Web Server** – The service that provides both administration, as well as, the deny pages shown when a subscriber is blocked from accessing a site.

- **Reporter** – The service that logs each subscriber request and generates reports on both general network statistics and individual subscriber usage

In smaller deployments, some or all service components can be combined on a single physical platform. In larger deployments, separate Interception Device, Policy Server, Web Server, Database or Reporter platforms are deployed based on performance requirements.
Network Service Components

The following diagram depicts how an Interception Device intercepts network traffic. Once a user request is picked up (1), the Interception Device sends the request to the Policy Server for allow or deny ruling (2). The Policy Server finds a category for the request, compares the category to the policy, and returns a ruling to the Interception Device (3). While the Interception Device carries out allow or deny rulings, the Policy Server logs requests with the Reporter (4).

Interception Device

The Interception Device can be deployed in the following different methods:

- Default Gateway Router (in-line solution) – using this deployment method, the Interception Device monitors and filters traffic as it travels from one sub-net to another.

- Transparent Network Bridge (in-line solution) – using this deployment, the Interception Device requires that all workstations on a network have their default gateway configured to send traffic to the Interception Device. This type of implementation involves configuring DHCP services or IP workstation settings to use the Interception Device as a default gateway, whereby it acts as a router.

- Pass-by filtering (not an in-line solution) – Using a switch to that is capable of copying and forwarding packets (also known as an IDS or Port Mirroring switch), packets will be copied and sent to the Interception Device simultaneously for identification. Should the Policy Server determine that the request is to be blocked, the Interception Device will inform the switch to cancel the request and serve up a deny screen.

Policy Server

The Policy Server is the core service component. It receives outgoing requests from the Interception Device, categorizes the request, maps the requests to a policy, and determines whether the request should be allowed or blocked. If the Policy Server is unable to make a categorization decision locally (using its own cache and rules), it communicates with upstream CNS devices to assign a category for the requested URI.
The Policy Server is not normally in-line with the network traffic. It can be hosted locally or remotely. The Policy Server records request results in the Reporter log.

In its smallest deployment, the Policy Server is a single hardware platform running the Web Server for administrative functions and the Reporter for reporting services. In an ultra-small deployment, the Interception Device can also be run on the same hardware platform as the Policy Server.

In larger deployments, the Policy Server consists of multiple platforms and several separate Web Servers and Reporter platforms either as virtualized servers or integrated with load balancing network appliances.

For example, a CISCO Content Switch can be used to load balance traffic across the Interceptor Devices, as well as, Policy Servers, ensuring 99.999% availability.

**Web Server**

The following diagram depicts how an administrator uses the Web Server to change system and Policy Server configuration settings (1). The Web Server sends updates settings the Database (2) and then the Database notifies the Policy Server (3) to retrieve the new configuration settings from the Database (4).

---

---
The following network diagram depicts a logical expression of how a Web Server service component responds with a deny page when a subscriber is blocked from accessing a site:
**Reporter**

The Reporter can be used to generate and email reports in real-time or automatically on a daily, weekly or monthly basis for individual subscribers or groups of subscribers. The Mail Server below can be an additional service component on the Web Server or it may be completely separate from the Web Server.

The following network diagram depicts how the Reporter is used to generate and retrieve usage reports. First, the user requests a report using the Web Server (1), which notifies the Reporter to generate the report (2). While creating the report, the user can view the report directly from the Web Server (path 3a) or opt to have the report sent by email (path 4b).

---

**3rd Party Interceptors**

The policy server can be integrated with various 3rd party firewalls and caching platforms to provide extremely simple deployment of packet filtering and web security services into existing customer network environments.

Most firewalls and caching platforms (Cisco, Juniper, Bluecoat and Microsoft ISA) have the ability to forward duplicate requests or to query the Netsweeper system directly with the aid of plug-ins. With a hosted Policy Server, service providers can offer packet filtering and web security to customers that have firewall or caching platforms capable of forwarding a duplicate of the HTTP request traffic or query the Policy Server directly with the use of plug-ins – with no more than a couple of minor configuration changes to the customer’s existing firewall or caching platform.

For example, virtually all education, government and corporate environments employ firewall or caching platforms. Generally, these platforms have the ability to operate in pass-by mode, where the HTTP requests are copied to an external IP address. If this is the IP address of a Policy Server, the request will be categorized, logged, and ruled on (allow or deny). This provides an opportunity to provide packet filtering, web security, monitoring, and reporting with no additional hardware required at the customer’s site – all that is typically
required are two configuration changes: one to turn on pass-by mode and one to specify the IP address to send the duplicate request or configure the plug-in.

The following network diagram depicts an implementation example with multiple 3rd party interceptors:

![Network Diagram](image)

**Determining Physical Network Location**

If separated onto multiple hardware platforms, service components can be distributed across network infrastructure environments to optimize network performance. For example, Interception Devices can be placed in each of several smaller network environments and can poll a centralized Policy Server architecture, which is designed to handle packet filtering, web security, policy management, logging and reporting for each of the smaller networks simultaneously.

In a single-location deployment, Interception Devices can be placed in-line with the flow of traffic (pass-through filtering) and all of the local components can be placed within the network. However, it is possible to isolate all of the
Netsweeper components within a DMZ (“Demilitarized Zone”, an externally-accessible network area that is somewhat isolated from internal network resources for security purposes). It is also possible to place some service components on the network while leaving others in the DMZ.

A common method of achieving this is to use an existing firewall as a 3rd party interceptors, which then processes the request and asks the Policy Server for a ruling. If the Policy Server returns a deny ruling before the request response is received, the user is redirected to a deny page on the Netsweeper. If the Interceptor is connected to a port mirroring or tree spanning switch then this type of filtering is called pass-by filtering since the traffic is never passed through or held up by Interceptor components. The following network diagram depicts this scenario:
Deployment Examples

Service providers can choose from a wide variety of flexible deployment options depending on specific network platform connectivity, performance, and subscriber customer base requirements. The following examples are only a very small subset of potential deployment options.

Service Provider Core Network

In this extremely high demand service provider core network deployment, multiple Interception Devices and Policy Servers are installed to accommodate an extremely high volume of network traffic and concurrent connections, as well as to provide availability and failover support. A Deep Packet Inspection (DPI) platform is also used to increase network performance. In this example, inbound traffic does not travel through the Interception Devices. However, a bi-directional packet filtering and web security solution can be also be implemented in service provider core network environments.

Also in this example, load balancing and redundancy is performed by the DPI solution. Alternatively, an OSI Layer 4 switch could be used to manage load balancing and availability. The Web Server and Database are included on the Policy Server, but could also be separated to improve availability and performance with redundant and failover configurations.
High Demand Network

In this high demand network deployment, multiple Interception Devices and Policy Servers are installed to accommodate a high volume of network traffic and concurrent connections, as well as to provide availability and failover support. In this example, inbound traffic does not travel through the Interception Devices. However, a bi-directional packet filtering and web security solution can be also be implemented in high demand network environments.

Also in this example, an OSI Layer 4 switch manages load balancing by routing or forwarding URI requests on HTTP or HTTPS ports to available Interception Devices and Policy Servers. Alternatively, a virtual server environment could be used to manage load balancing and availability.

Additionally, a standalone Reporter is used to provide independent processing power to log each user request and generate reports on both general network statistics and individual network usage. Multiple Reporters could be deployed in a virtual server or load balanced environment to provide redundancy and fail over capabilities.

And finally, the Web Server and Database are included on the Policy Server, but could also be separated to improve availability and performance with redundant and failover configurations.
Estimating Platform Requirements

To define a deployment strategy, the following network variables can help determine estimated platform requirements:

- **Interception Devices** – the total amount of network traffic to filter measured in Gbps
- **Policy Servers** – the average number of concurrent Policy Requests

<table>
<thead>
<tr>
<th>Server Type</th>
<th>Performance Mbps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dell PowerEdge R900 w/Regular Intel Cards</td>
<td>400</td>
</tr>
<tr>
<td>Netsweeper Appliance</td>
<td>2,000</td>
</tr>
<tr>
<td>BlueCoat</td>
<td>600</td>
</tr>
</tbody>
</table>
SUPPORT AND MAINTENANCE

Netsweeper offers maintenance, support and service programs that extend our product life span and maximize uptime.

- Basic Warranty Support
- Advanced Server Replacement
- Advanced Parts Replacement
- Advanced Parts Replacement with On-Site Technician
- Anytime On-Site
- Anytime On-Site with Advanced Troubleshooting
- Technical Support Services

Basic Warranty Support

Netsweeper guarantees that every system sold functions properly — 100% free from workmanship defect under our Basic Warranty Support terms for two (2) years after receipt of product. Extended (optional) warranties are also available to Netsweeper customers who wish to lengthen warranty periods.

Components integrated into systems are under warranty for 30 days. However, many of these components carry longer warranties issued by the original manufacturer, which we freely pass along to our customers.

Basic Warranty Support also provides direct access to technical (troubleshooting) staff either by e-mail, telephone or online. Technical support by telephone is available between 8:00 AM and 5:00 PM EST on weekdays (excluding holidays). Our on-staff experts are always ready to answer questions and resolve problems. If after troubleshooting any damaged or inoperable equipment must be returned, we quickly repair or replace the equipment and expedite its return to service. For equipment deemed out-of-warranty, repair and return service is handled on a time and materials basis.

Advanced Server Replacement

Netsweeper offers Advanced Server Replacement (ASR) as an optional service designed specifically for fast system substitution. With ASR, multiple pre-configured systems can be stocked and made ready to ship in the event of field unit malfunction or damage. Field replaceable units (FRUs) are provided as well for serviceable components such as hot-swap power supplies and hot-swap hard drives. This plan is popular among customers who purchase and deploy high volumes of identical systems. ASR systems are shipped by priority/overnight freight. Forward stocking is also available as an ASR option.
Advanced Parts Replacement

Many customers prefer our optional Advanced Parts Replacement (APR) program, which extends the warranty on parts for a minimum of one (1) year to a maximum of three (3) years. Problems received with APR status are given workflow precedence. After any failed part has been diagnosed and identified, a replacement part is shipped via priority/overnight freight Monday through Friday (excluding holidays). Netsweeper assumes all freight charges for replacement parts. This program is great for customers that have add-in components such as telephony boards and can save critical time as well as simplify the tracking and processing of replacement components.

Advanced Parts Replacement with On-Site Technician

When technical issues require professional on-site assistance, Advanced Parts Replacement with On-Site Technician delivers experienced technicians to your door during local business hours (between 8:00 AM and 5:00 PM). For problem-free installation or equipment replacement, our on-site technicians take the guess-work out of installation. Optionally available is the forward stocking of replacement parts, which will ensure same-day arrival (in major metropolitan locations) within four hours of your support request.

Anytime On-Site

When 24×7×365 availability is mission critical, our Anytime On-Site program gives you full-time service and support — weeknights, weekends and holidays included. This comprehensive program includes all the components of APR with On-Site Technician and dispatches a qualified technician to your location (any time of day) in as few as four hours after the replacement parts are delivered onsite. Forward stocking of replacement parts is available as an option to enable same-day arrival of parts for on-site technicians.

Anytime On-Site with Advanced Troubleshooting

For the most all-inclusive, hands-on support, service and troubleshooting program available, many customers enroll in the Anytime On-Site with Advanced Troubleshooting program. This program offers the ultimate insurance against long-term downtime and guarantees that a technician is dispatched (within four hours of the support request) to your facility where they can quickly diagnose and solve equipment problems. If necessary, our technicians will order and install replacement parts and/or systems that arrive by priority/overnight freight. Forward stocking is optionally available under this program. If your application warrants fail-safe operation, regular and timely maintenance, or you need top-line support services, Anytime On-Site with Advanced Troubleshooting is the program of choice.
Technical Support Services

Technical Support Services provide customers with access to an experienced staff of customer service professionals and technical support specialists. Trained and certified technicians are available during standard business hours or 24×7×365 (depending on your program) to provide installation, troubleshooting, repair and basic configuration support for Internet security, storage, network or telecommunications applications and systems. These services are available by phone, email or through the self-service web portal.

In addition to offering diagnostic and repair services on products covered by our Support and Maintenance programs, Netsweeper offers the ability for OEM’s, ISV’s and partner companies to leverage its existing support infrastructure and provide Level 1 through Level 4 technical support and diagnostic services. Netsweeper can handle service requests and work to diagnose, repair and resolve technical problems that can arise during installation and configuration of the equipment and our application. Netsweeper can customize support service plans as needed for customers.
SPECIFICATIONS

Recommended Carrier Grade Platform

- Form Factor – NEBS Level 3 certified 1U carrier-grade server
- Processor – Quad-Core Intel Xeon L5410 or Dual-Core Intel Xeon LV5148 or LV5128
- Memory – 4 GB memory per DIMM (six DIMM slots) Fully-buffered DIMM technology at 533 and 677 MHz or faster.
- Chipset – Intel 5000P Memory Controller Hub (MCH) and Intel 6321ESB I/O Controller
- Storage – Drive bays for up to 3 hot swap 2.5-inch SAS drives; external x 4 SAS connection, software RAID 0, 1 and hardware RAID 0, 1, 5
- Expansion – One full-length, full-height super slot: PCI-X or PCIe x 8
- Network – Integrated four-port 10/100/1000 Mbps Ethernet; connectors located on rear (Optional 10 GbE Fiber Adapter)
- Power – Dual redundant hot swap 450W AC or -48 V DC power supply
- Cooling -- Two 40x40x56nm dual-rotor fans, One 40x40x28nm single-rotor fan for PCI area airflow, Four 40x40x56nm dual-rotor fans for CPU-memory-HDD area airflow; Intel Active Air Flow control, Intel Server Management for fan failure detection
- Operating system – Netsweeper 2.6
- Compliance – AC and DC NEBS Level 3 compliant, ACPI BIOS, PCI-X, USB v2.0, Extended ATX motherboard and ATX PSUs, ETSI standards compliant (DC input only), RoHS compliant

Packet Filtering and Web Security

- 98 categories and protocols – 8 of which are security related
- SSL encrypted URI scanning and categorization
- Language and content aware – English, German, Portuguese, Spanish, Japanese, Russian, Arabic, French, Polish, Turkish (vast coverage of other international sites)
- Over 3 billion active URIs categorized and growing by approximately 10 million per day
- Auto-adjusting cache
- Over 200,000 requests per second with low resource utilization
- RADIUS, LDAP, Active Directory, eDirectory and other subscriber authentication systems
CONCLUSION

Netsweeper provides the industry’s most advanced intelligent core and edge packet filtering and web security services that are proven to be fully compatible with service provider billing and provisioning integration, and subscriber authentication, authorization and accounting strategies.

Netsweeper offers service providers unparalleled flexibility to categorize content and offer world class policy management and web security services to subscribers.

Netsweeper has extensive industry experience in helping service providers around the world maximize profitability and protect the security of their data network infrastructure.

With Netsweeper, service providers can be confident that they are working with the market leader in advanced packet filtering and proactive web security services.