

Overview of Zscaler Services

Emerging Web 2.0 Challenges for User-Initiated Traffic

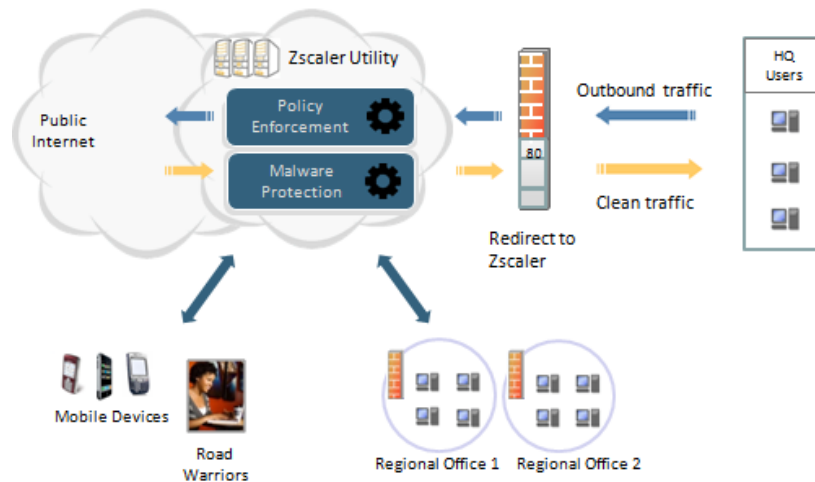
Most of today’s security products—such as firewalls, VPN, IDS/IPS—protect corporate networks and servers from threats coming from the Internet. Newer threats, such as bots, phishing, and malicious active content, target end-users accessing Internet resources and infect corporate networks. Other than deploying caching and URL filtering products, corporations have done very little to inspect user-initiated traffic and protect their users.

Web 2.0 applications, such as social and business networking, create both opportunities and challenges. They help create communities of interest for marketing, but also create risks when users inadvertently download malicious content, or create liability when employees publish inappropriate or confidential content on blogs and social networks. Road warriors and smartphone users further exacerbate this problem—their access to the Internet often bypasses all security controls.

Zscaler In-the-Cloud Service

Imagine a world in which each company *generated its own power*. In addition to purchasing and installing generators, organizations would have to hire staff for the maintenance and repair of those generators. By contrast, the plug-and-play electricity used today seems incredibly convenient and cost-effective. Similarly, the cottage industry of security will slowly disappear; organizations are moving away from buying and maintaining numerous security appliances on-site in favor of an in-the-cloud security service. The vibrant growth of companies such as salesforce.com and NetSuite has proven that software-as-a-service (SaaS) is a viable model.

Zscaler enriches user experience for Internet access, while providing risk mitigation and policy enforcement for CEOs and CISOs through its in-the-cloud service. Organizations do not need to purchase, deploy, or manage countless point products. Companies simply define their corporate security, control, and compliance policy by accessing the Zscaler service.



Zscaler’s in-the-cloud utility enables seamless policy enforcement and malware protection for multiple locations, mobile devices, and road warriors.

The web traffic leaving the network firewall is easily redirected to one of the data centers in Zscaler’s global infrastructure. End user traffic bound for the Internet is allowed, blocked, or throttled based on an organization’s policy. As the browser retrieves the web pages, Zscaler scans it for a range of malware threats

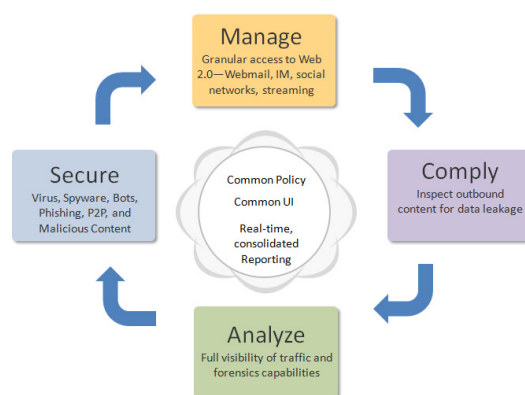
and delivers clean traffic to the end user. Zscaler service is not a firewall, intrusion prevention, or email security solution—which are focused on protecting either the network or corporate servers from outside-in threats. Zscaler’s focus is to protect the end user, who is accessing Internet resources.

Most organizations have multiple Internet gateways; each gateway is a potential entry point for an attacker and requires multiple point products to secure. Zscaler’s integrated and comprehensive functionality provides security and control for any user, any device, at any location without the need for multiple point products. Traffic from each firewall or device is simply redirected to the Zscaler cloud. This is the only practical approach to secure road warriors and mobile devices.

The Zscaler cloud eliminates the cost of acquiring point products, the cost of deploying them, and the costs of maintaining them. Organizations pay an annual subscription fee to use the service. Zscaler allows IT administrators and security analysts to focus on defining and enforcing company policy, rather than spending their precious time managing and updating appliances.

Zscaler Functionality

Zscaler provides an integrated, best-of-breed, and comprehensive functionality. It allows organizations to create common, granular policies for various areas. It has an intuitive user interface, so that use of the service literally requires no training. There are four key areas of functionality: secure, manage, comply, and analyze.

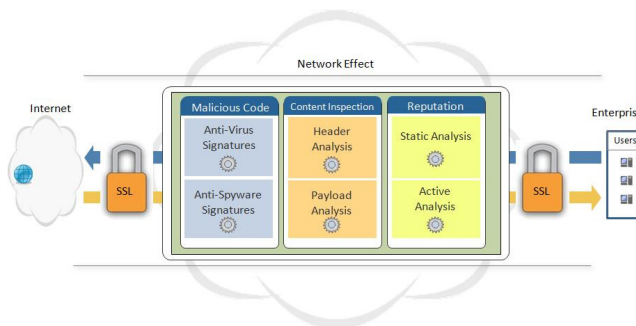


I. Secure

Security threats have evolved from desktop-based viruses to email-based worms, and now are largely becoming browser-based threats. Zscaler inspects all outbound and inbound web traffic to protect enterprises from these threats.

Viruses & Spyware: The Known Threats

Zscaler inspects and protects against known viruses and worms using signature and heuristic technologies. Zscaler’s architecture provides inspection at many times the speed of most competitive products, ensuring full protection without introducing latency. In addition, spyware is a pervasive and significant security risk. Zscaler anti-spyware detects and stops a range of spyware, including malicious Trojans, system monitors, keyloggers, and adware.



Zscaler’s single-scan, multi-action (SSMA) technology minimizes latency, while providing multi-layered security.

Advanced Threats: Bots, P2P, Malicious Content and Phishing

Zscaler inspects web traffic for new and emerging threats such as botnets, which use end users’ computers as a virtual army to launch a variety of attacks. It also detects phishing sites, which attempt to social engineer end users into revealing confidential information. Zscaler protects users from receiving malicious content from today’s Web 2.0 pages, which use active content—such as ActiveX, Ajax, Flash, or JavaScript—which can easily hide malicious code. Zscaler can also detect and block peer-to-peer traffic (P2P), which can consume large amounts of bandwidth and create security and liability risks.

Decrypting SSL Traffic

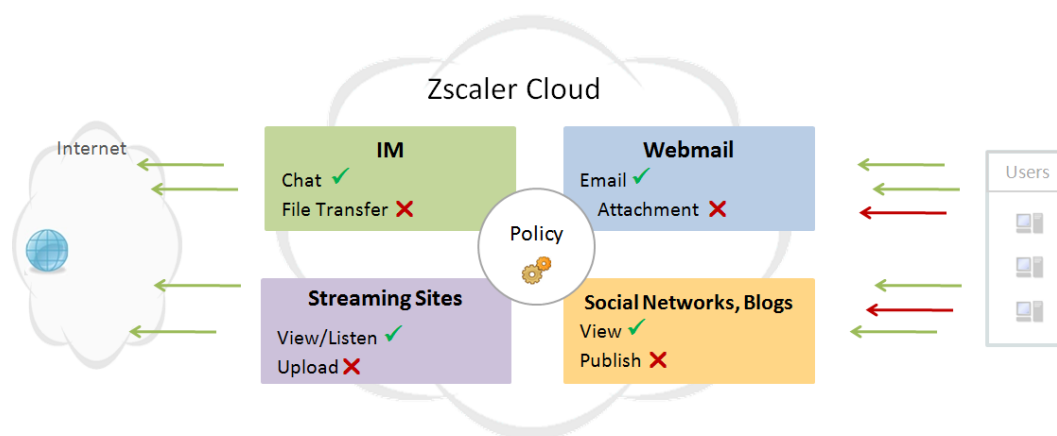
Web traffic is increasingly being encrypted using the SSL protocol. If an organization selects SSL decryption policy, Zscaler allows that organization to decrypt SSL traffic to detect and block hidden malicious content or outgoing sensitive information.

Benefits: Full Protection against Inbound and Outbound Threats

The Zscaler cloud becomes the first line of defense against known and zero-day threats—blocking them before they even reach your network. Zscaler has the unique benefit of network effect due to its in-the-cloud architecture with a global infrastructure, allowing it to detect and protect against outbreaks from any part of the world as soon as they occur.

II. Manage

Web 2.0 trends—from social and business networks to user-generated content—create both opportunities and challenges for today’s organizations. Users are no longer just the consumers of web content; they are now the creators. This provides opportunities to create communities of interest for marketing and to increase productivity. Unless controls are put in place, however, this can also create liabilities for organizations when their employees publish inappropriate or confidential content on blogs and social networks. Furthermore, the use of rich multimedia applications, such as audio and video streaming technologies, can negatively impact the network performance of the entire office—instantly affecting productivity.



Zscaler’s high-speed, dynamic content classification improves resource utilization by providing the granular control demanded by Web 2.0 applications.

URL Filtering with Dynamic Content Classification

Internet access has traditionally been controlled using a URL filtering database, which consists of 15-20 million blacklisted domain names and URLs. But Web 2.0 is changing the nature of the Internet. Previously, only established organizations had web sites, and their web pages were fairly secure. Now, much of the content on the Internet is dynamic and user-generated. This evolution in web content has limited the value of static URL filtering technologies.

In addition to leveraging a URL filtering database for category classification, Zscaler has pioneered a new dynamic content classification technology. Uncategorized Web pages being downloaded are scanned on the fly at high speed, categorized, and handled based on company policy. Zscaler provides 80 pre-defined categories that are grouped into 30 super-categories. Super-categories are further grouped into 5 URL classes: security, legal liability, productivity loss, bandwidth loss, and business use.

Zscaler allows organizations to create granular policies based on location, department, individual employee, and time and volume quotas. Furthermore, Zscaler provides the option of SafeSearch, which filters web, image, and video searches for Yahoo! and Google Search.

Providing Managed Web 2.0 Access

Zscaler provides a unique solution to manage access to Web 2.0 applications. The answer is not to block access completely, nor is it to allow unrestricted access. The solution lies in providing managed access. Zscaler offers progressive organizations to create flexible and granular web access policies by action, location, and group. For example, organizations may choose to:

- Allow selected Webmail applications, but restrict file attachments, which can risk data leakage.
- Allow all employees to access and view social networks for an hour a day, with the exception of marketing, which can view & publish on social networks such as Facebook to promote communities of interest.
- Allow employees to use videos & audio sites, such as Youtube, for a maximum of 50 MB per day, but prohibit uploading content during office hours.
- Allow certain instant messaging (IM) applications for chat, but prevent file transfers.

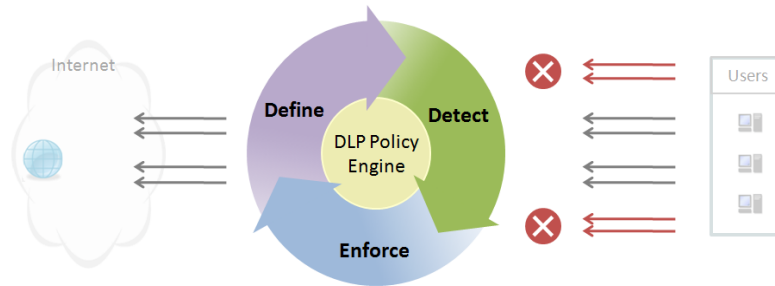
Benefits: Maximize Your Resources, Reduce Liability

Zscaler allows organizations to leverage Web 2.0 access to promote sales and increase customer satisfaction while eliminating Web 2.0 liabilities and challenges. It improves the utilization of network resources, by minimizing the use of bandwidth-hog applications, and of human resources, by limiting time-wasting activities and improving employee productivity.

III. Comply

As the traditional perimeter is vanishing, with enterprises connecting to their customers and partners, data leakage is becoming an expensive, burdensome problem. Employees, whether their intent is innocent or malicious, can easily send a Webmail or IM with confidential information. Information can be posted on social networks and blogs instantaneously. Private information, such as consumers' Social Security and credit card numbers, is protected by government regulations and leakage creates legal liabilities and harms brand reputation. Further, leaks of sensitive company information risk financial loss.

Several companies have emerged to offer specialized solutions to prevent data leakage. These solutions often require extensive implementation and consulting services. They are also just another point solution to be added to an already-crowded perimeter gateway. Not surprisingly, less than 5% enterprises have deployed data loss prevention (DLP) solutions today.



Zscaler DLP solution allows organizations to define and enforce a flexible policy to prevent data leakage.

Zscaler Enforces Compliance Policy

The Zscaler solution, which allows enterprises to detect and protect against data leaks, can be deployed in minutes. Zscaler provides full inspection of all HTTP/HTTPS traffic leaving the organization. Specifically, our technology inspects two types of violations:

- *Regulatory compliance* by state or federal governments, or other standards bodies, often pertaining to personal or private consumer information. Examples include regulations such as HIPAA, GLBA, PCI, or SOX.
- *Company sensitive information* may include sales data, pricing information, or intellectual property such as source code.

Granular Policy, Flexible Dictionaries and DLP Engines

Zscaler service uses DLP engines and dictionaries that are easy and flexible. Enterprises can define custom dictionaries and engines in addition to the pre-defined dictionaries and engines provided by Zscaler. Because of Zscaler's in-the-cloud architecture, customers do not have to deploy DLP boxes at every Internet gateway. Policy definition is intuitive but powerful, offering granular control over specific users, locations, and applications (Webmail, social networks, etc).

Benefits: Accurate Detection & Easy of Deployment

Zscaler provides an integrated DLP solution with the highest accuracy of detection. The high-performance system does not introduce any latency. Finally, deployment takes minutes rather than months required by other products.

IV. Analyze

Over 70 % of the total enterprise traffic leaving the firewall is HTTP or HTTPS traffic. This traffic generates massive amounts of logs: the web traffic of a typical Fortune 500 company generates 10-40 Gigabytes of logs *everyday*. Companies with multiple Internet gateways generate logs on each gateway proxy, which do not provide a consolidated view of overall corporate Internet activity. There are no easy tools that provide either consolidated reporting or specific data mining.

Most companies need to store web logs for at least a year. Current web log solutions use relational databases, which do not scale to handle such large amounts of data storage and are too slow to access and analyze information. In addition, companies spend a great deal of money on storage media to save logs that cannot be effectively retrieved or used.

Big-Picture View & Data Mining

Zscaler's web log technology, NanoLog, can handle enormous amounts of data for storage and analysis. It allows organizations to analyze information on Internet use, such as employee activity, Webmail and attachments sent, information published on social networking sites, or instant messaging communication with partners or competitors.

Zscaler allows companies to mine logs for investigative purposes, either for regulatory reasons or internal inquiries. Companies can see a drill-down of activities of specific periods of time, employees, departments, locations, and more. For example, which employees at the Atlanta office sent an IM message with an attachment, including confidential information, to a competitor? In addition to analyzing specific behavior, Zscaler gives organizations a better understanding of broad traffic trends, which provides insight into anomalous behavior and planning for bandwidth and network requirements.

Benefits: Flexible & Powerful Reporting and Analysis

Zscaler provides organizations a flexible & powerful system to view the broad trends and traffic patterns of Internet activity, as well as drill down to specific activities. It reduces the cost for web log retention and offers high-speed web log retrieval. In addition to helping fulfill regulatory obligations, Zscaler offers organizations a comprehensive view of Internet activity for planning future network requirements.

High Functionality, Low TCO

Compared to competitive solutions, Zscaler's in-the-cloud service offers a lower total cost of ownership.

- First, a SaaS service does not require an up-front capital investment. Appliance-based and software-based solutions require organizations to purchase and deploy appliances or to license and install software.
- Second, the deployment of appliances and their associated software is costly, both in terms of money and time. IT personnel have to be trained, and appliances have to be shipped and installed. An in-the-cloud solution takes minutes to deploy and Zscaler's intuitive dashboard requires no training.
- Third, traditional solutions require organizations to deploy at least two appliances per Internet gateway as a failover. For a corporation with multiple gateways, the costs of failover appliances are burdensome. Zscaler's centralized network consists of Internet gateways in all major, global locations. Failover infrastructure is our responsibility—if one gateway fails, traffic automatically travels through a nearby gateway.
- Lastly, traditional solutions require the hidden burden of on-going maintenance. Significant administrative support must be provided to ensure that appliances are up, running properly, and updating releases, patches and signatures. By freeing up IT personnel, Zscaler allows organizations to focus their limited IT resources on policy enforcement.

The Zscaler service is the only solution that provides a comprehensive, best-of-breed, and integrated functionality at a low TCO. Only Zscaler provides a complete suite of in-the-cloud services: malware protection, dynamic, application-based managed control; compliance; and consolidated reporting and forensics.



Zscaler, the Zscaler Logo, and NanoLog are trademarks of Zscaler, Inc. in the United States. All other trademarks, trade names or service marks used or mentioned herein belong to their respective owners. August 2008.