

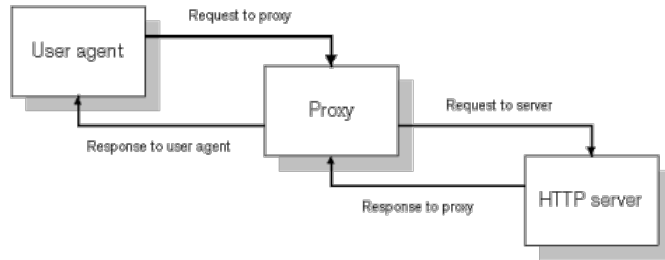
Introduction

Zscaler services enable any end user, from any place, using any device, to experience a rich Internet experience while enforcing security and business policy. Rather than buying appliances such as web proxy, URL filtering and anti-virus gateways at each Internet egress point, Zscaler provides risk mitigation and policy enforcement for businesses through a globally distributed cloud infrastructure.

To leverage Zscaler’s service, companies simply define their corporate security control and compliance policy by accessing the Zscaler administration portal (once provisioned) and redirect all web traffic leaving their network to one of the 40+ data centers in Zscaler’s global infrastructure. Based on an organization’s policy, traffic is blocked, throttled, or allowed to access the Internet. As the browser retrieves the web pages via HTTP proxy methods, Zscaler scans it for a range of malware threats and delivers clean traffic to the end user.

HTTP Basics

The application protocol used by a browser to view webpages is Hypertext Transfer Protocol (HTTP). HTTP is a request/response protocol; your web browser computer sends a request for content (e.g. "get me the file 'cnn.com/index.html'"), and the web server sends a response ("Here's the file", followed by the file itself). Once the container page itself has been retrieved, your browser processes the entire file and sends out series of requests for all the component parts (additional sourced text/html, images, active content via scripts, etc.).



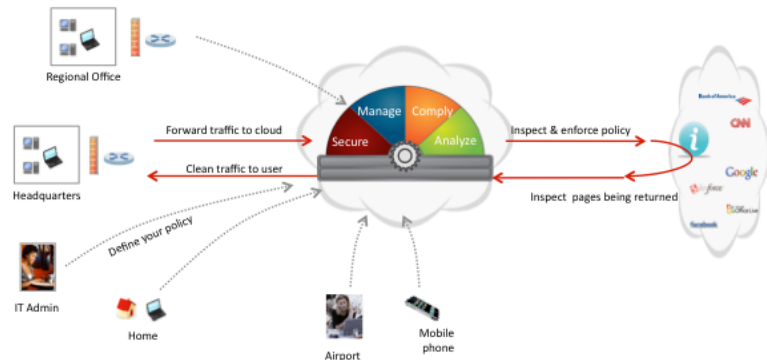
For every request generated by the browser, a corresponding response is generated and sent back by the content server.

When a proxy is introduced into this workflow, the proxy acts as a broker; the client makes the requests to the proxy and the proxy gathers this content on behalf of the client prior to sending it back to the client. This gives the proxy the ability to inspect or process the content as it passes through prior to the client receiving

it. Setting up the client to use a proxy, thereby redirecting all requests, is referred to as traffic forwarding.

Traffic Forwarding

Forwarding traffic to the Zscaler cloud is extremely simple. Zscaler requires no hardware or software in the customer’s network or end users’ workstations to direct web traffic to its cloud. Using existing infrastructure, traffic is forwarded at the network layer to one or more of the Zscaler Enforcement Nodes (ZENs).



There are primarily four methods for doing this:

- **GRE Tunnels:** Rules on a firewall or edge router are created to provide a secure tunnel to a specific ZEN. This is the preferred method of traffic forwarding because it supports both HTTP and HTTPS traffic, as well as fail-over to a second (or third) ZEN (should the first enforcement node become unavailable for any reason).
- **Proxy Chaining:** An existing internal web proxy (e.g., Squid forward proxies) is used to forward HTTP traffic to a ZEN.
- **Port Forwarding:** Many firewalls allow port 80 traffic to be forwarded to another host—in this case a ZEN.
- **Web Browser Proxy Configuration:** For those users outside of the corporate network, the browser itself can be configured to forward its HTTP/HTTPS requests to a ZEN.

Each of these methods is described below.

GRE Tunnels

GRE Tunnels are configured on the organization’s perimeter firewall or edge router. The tunnel originates at the edge and terminates at a ZEN within Zscaler’s cloud. For redundancy and failover, two or more tunnels may be configured on each external device. If connectivity through one tunnel goes down, the router will automatically switch to the next ZEN. Typically, GRE tunnels use “keep-alive” packets to determine if a tunnel is up or down.

- Pros:**
- Multiple tunnels offer full redundancy
 - Users cannot bypass Zscaler
- Cons:**
- Users off the corporate network are not protected by Zscaler

Forward Proxy Chaining

You may use an existing web proxy to “chain” or forward traffic to a ZEN. In this configuration you would modify your existing web proxy to forward all traffic to the Zscaler cloud. This varies between different platforms but is generally a simple configuration change. Please refer to your existing proxy documentation for further information on how to configure this.

- Pros:**
- Easy to setup
 - Multiple rules offer full redundancy
 - Supported by every major web proxy
 - Users cannot bypass Zscaler
- Cons:**
- Users off the corporate network are not protected by Zscaler

Port Forwarding

Depending on which firewall your organization has deployed for your environment; you may have the option to work with Firewall Port Forwarding. This mechanism allows you achieve the same basic functionality as GRE tunnels on much simpler network devices. While it may be a simple straightforward solution, it does come with several drawbacks: no automated fault detection nor HTTPS support.

- Pros:**
- Easy to setup
 - Supported by every major firewall
 - Users cannot bypass Zscaler
- Cons:**
- Only supports HTTP traffic (not HTTPS)
 - Requires a manual change if the primary Zscaler gateway is unavailable
 - Users off the corporate network are not protected by Zscaler

Web Browser Proxy Configuration -- PAC Files

PAC (Proxy Auto-Configuration) files are text files containing JavaScript, a high-level programming language. The PAC files specify which proxies should be used and under what circumstances. PAC files may be hosted on each workstation, on an internal web server, on a server outside the corporate network or on Zscaler. Browsers’ simply require the address of the PAC file— they fetch the file at the address specified and execute the JavaScript contained within it.

- Pros:**
- All major browsers support PAC files
 - Easy to deploy via Active Directory
 - Users on and off the corporate network are protected by Zscaler
- Cons:**
- Users with admin rights may be able to install a non-standard browser attempting to circumvent Zscaler

Deployment Options

Below is a table of recommended deployment methods (P – Preferred; S – Supported; NS – Not Supported):

	GRE	CHAIN	PORT	PAC
Evaluation Phase	S*	P	S	P
Known Locations (Static IP)	P	S	S	S
Unknown Location/Mobile (Dynamic IP)	NS	S	S	P

*Supported but discouraged.