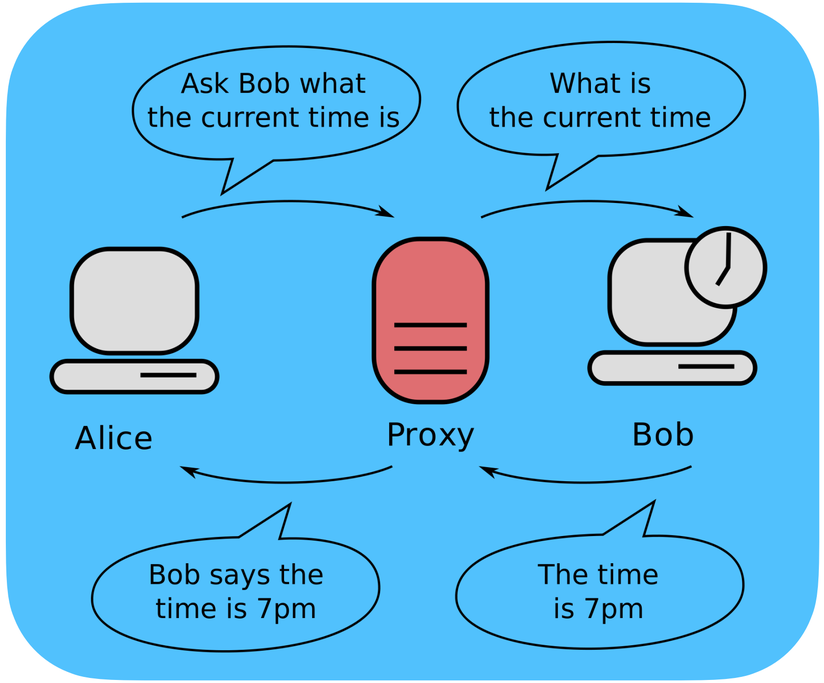
Proxy Services

Monitoring and Log Management

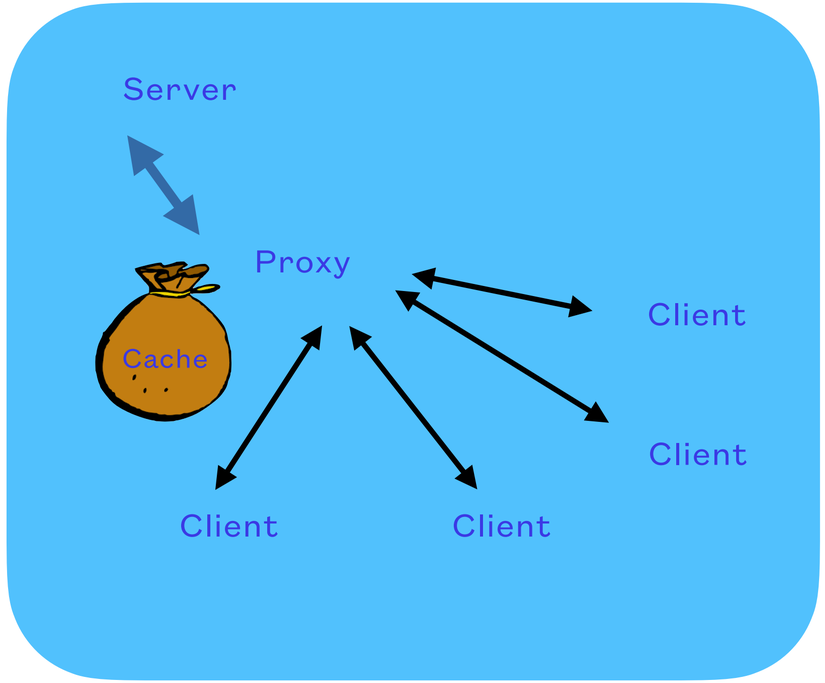
Concepts

- A proxy is something that performs a task for you
- A proxy server provides proxy services
- Various activities can be accomplished by proxy, including ftp, http, and other common internet communication tasks
- Encrypted connections using TLS/SSL require extra work to proxy
- It's MITM done to benefit the participants



Caching

- Proxy servers usually cache retrieved resources
- Servers can mark their resources as not cacheable, but proxies make their own decisions about what to cache and how long to keep the cached items
- Proxy software may or may not provide any way to control or view the cache(s)



Transparency

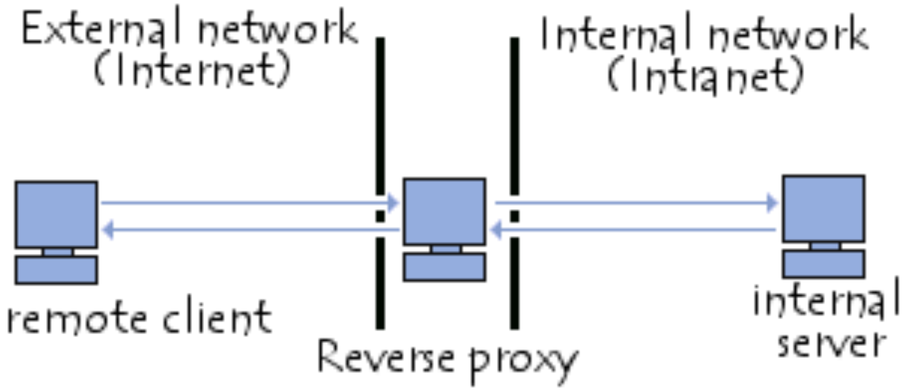
- Use of a proxy service can be explicitly configured or transparently configured
- A router or firewall running a proxy internally can intercept traffic without the client or server being aware of the intercept
- A proxy server can have traffic redirected to it by a router or switch for supported protocols

Transparent vs. Explicit

- Explicitly configured proxy services can allow for authentication to limit access to the proxy, and solve a number of less than obvious problems caused by transparent proxying (https://pharish.wordpress.com/2011/11/10/transparent-versus-non-transparent-proxying/ has some examples of how to know if transparency will cause trouble for you)
- Browsers can be configured for explicit proxy services manually, or using any of a number of client management tools, wget looks for an http_proxy environment variable

Proxy Server Applications

- A proxy server can be used for a number of distinct purposes
- It may be used to cache web resources locally for performance or data transfer reduction (basic, most common setup)
- It may be used to provide controlled access to protected resources (reverse proxy scenario)



Proxy Server Applications

- It may be used to conceal the identity of an end-user's host from the target server (the tor network uses a network of proxies to hide users)
- It may be used to restrict network traffic to specific choke points for traffic measurement and management purposes
- It may be used to modify or reroute traffic before delivering it to clients or servers (advanced proxy configurations)

Squid

- Squid is a proxy server which has been around since the mid 1990's (squid-cache.org)
- pfsense and others have the ability to run squid as part of the gateway, the pfsense package for squid3 bundles clamav for antivirus protection
- Consider blocking outbound direct traffic from the LAN to http on the internet to force internal hosts to use the proxy for http to the web

Squid Configuration

- Squid is highly configurable but can be run with very little customization from the defaults
- Only an acl and http_access are needed to get started as a simple http caching proxy, visible_host and http_port are other minor configuration options to use
- Port 3128 is the squid default, many browsers look for port 8080 as the default proxy service port - it is commonly used for content control software such as dansguardian, or e2guardian
- The /etc/squid3/squid.conf file has full documentation as comments, and is over 7000 lines long
- Changes to the squid.conf file require a squid restart

Proxy Testing

- Checking to see if your proxy is responding correctly can be done easily with wget
- Export the URL for your proxy in a variable called http_proxy, and use wget to retrieve a web page
- You can also test with a browser by setting the proxy in the browser preferences or settings

```
export http_proxy=http://proxyhost:3128

wget -O - icanhazip.com
```

Cache Management

- Squid includes some cgi code for accessing cache management information
- Enable access to it by adding a line in squid.conf for http_access allow localnet manager
- Some basic info can be retrieved by using the menu at http://proxyhost:3128/squid-internal-mgr/menu and replacing the word menu in that URL with a choice from the page retrieved by the menu URL

Reverse Proxy

- A reverse proxy accepts web client requests and transparently retrieves the resources from one or more servers before passing the response back to the client
- Reverse proxies can perform traffic control, flow monitoring, access control, load balancing, resource redirection, and content validation
- Apache's httpd can do it using mod_proxy and the ProxyPass directives - see https://httpd.apache.org/docs/2.4/howto/reverse_proxy.html
- So can many other web servers

Squid Logs

- Squid keeps logs in /var/log/squid3
- access.log shows traffic served
- cache.log gives cache management details

Web Proxy Services Lab

- proxyhost setup
- reverse proxy setup