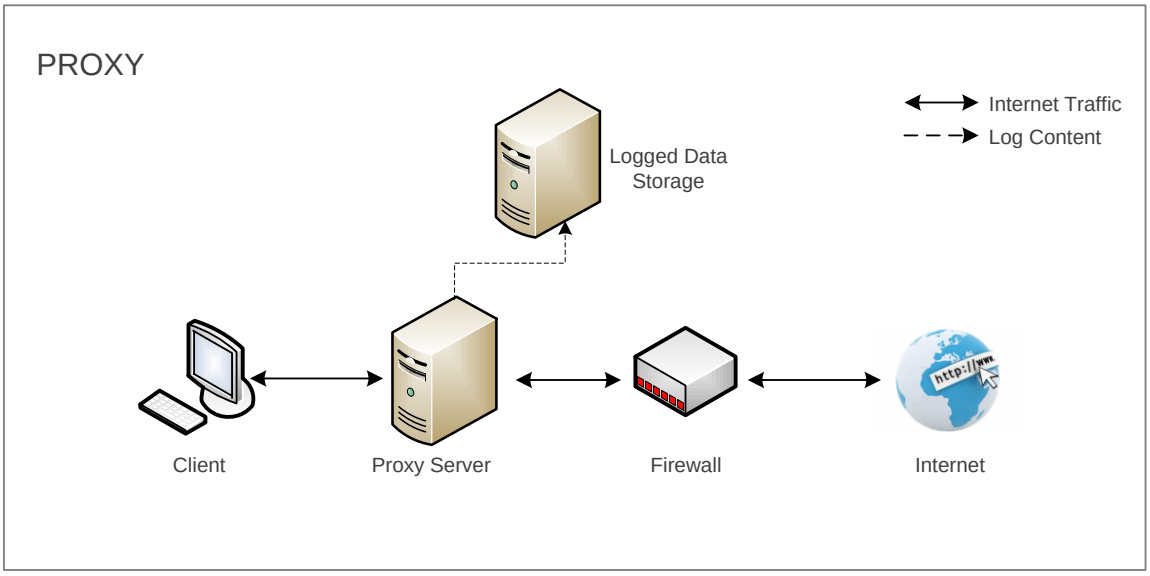
CASE STUDY || USER INTERNET MANAGEMENT DESIGN CHOICES

This paper provides a technical overview of the different design architectures used for User Internet Management (UIM). There are generally three architectures used in order to monitor and/or control the access to content available on the Internet: Pass-Through (Proxy), Pass-By (Sniffer) and Client-Server (Agent). Each has its advantages and disadvantages summarized in the following table and explained in detail below:

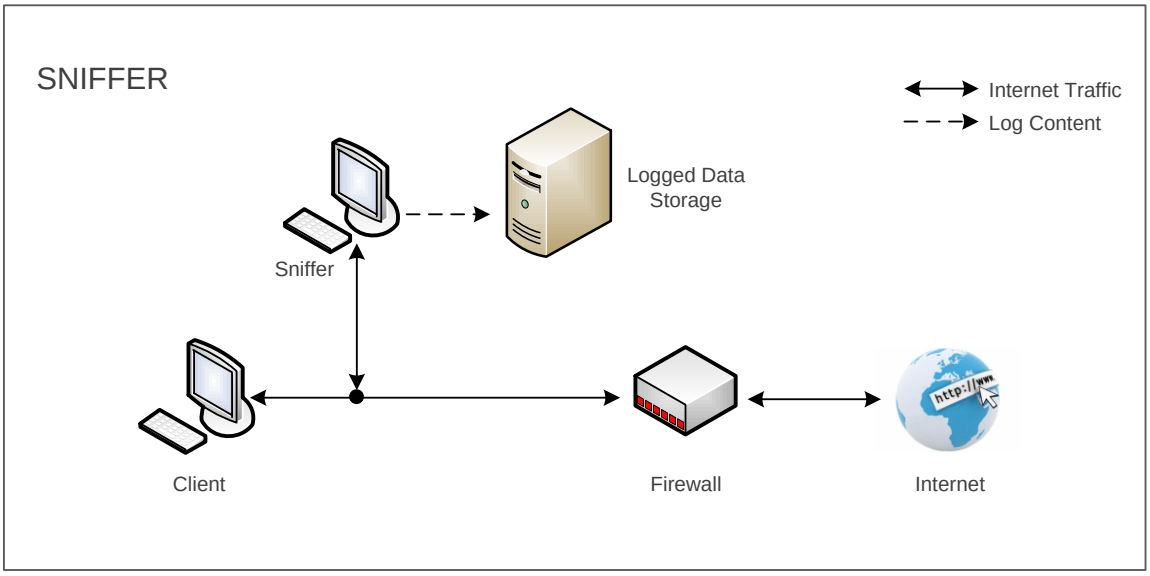
	Pass-Through (Proxy)	**Pass-By (Sniffer)**	**Client-Server (Agent)**
Single Point Install	✓		
Web Caching	✓		
Highly Secure			✓
Avoids Bottle Necks			✓
No Single Point of Failure Downing Network		✓	✓
Traffic Does not Need Redirection			✓
Controls On-Network Traffic	✓	✓	✓
Control Off-Network Traffic			✓
Multi-Protocol		✓	✓
Complexity Constant in Large Networks	✓		✓
Performance Scales in Large Networks			✓
Example	Websense	Surfcontrol	Pearl.Echo

Pass-Through



The Pass-Through architecture or proxy solution provides a central point of access to the Internet for all users. The proxy is normally a server, multiple servers, routers with imbedded UIM software or one or more "Internet appliances" – stand-alone server-like devices for targeted applications. A caching Web proxy provides a nearby store of Web pages and files originating on remote Web servers, allowing local network clients to access them more efficiently. When it receives a request for a Web page, a caching proxy looks for the content in its local cache. If the content does not exist in the proxy's cache, the proxy server retrieves it from the appropriate Internet server in order to satisfy the request and saves a copy in its local cache for future requests. The cache usually uses expiration algorithms to remove aged data. With a typical Web proxy, the client application must be configured to use the proxy. Alternately, an intercepting proxy combines a proxy server with a network address translation (NAT) device. Connections made by client browsers through the NAT are redirected to the intercepting proxy without client-side configuration. Though not foolproof, this helps prevent avoidance of UIM rules and reduces administrative issues created with configuring client browsers. Since requests to access Internet sites are sent from each workstation in the UIM environment, a decision about whether the site may be accessed can be made at the central point on the Pass-Through server. If a user requests a site that is determined to be off limits, the server returns a response to the user indicating that access is denied.

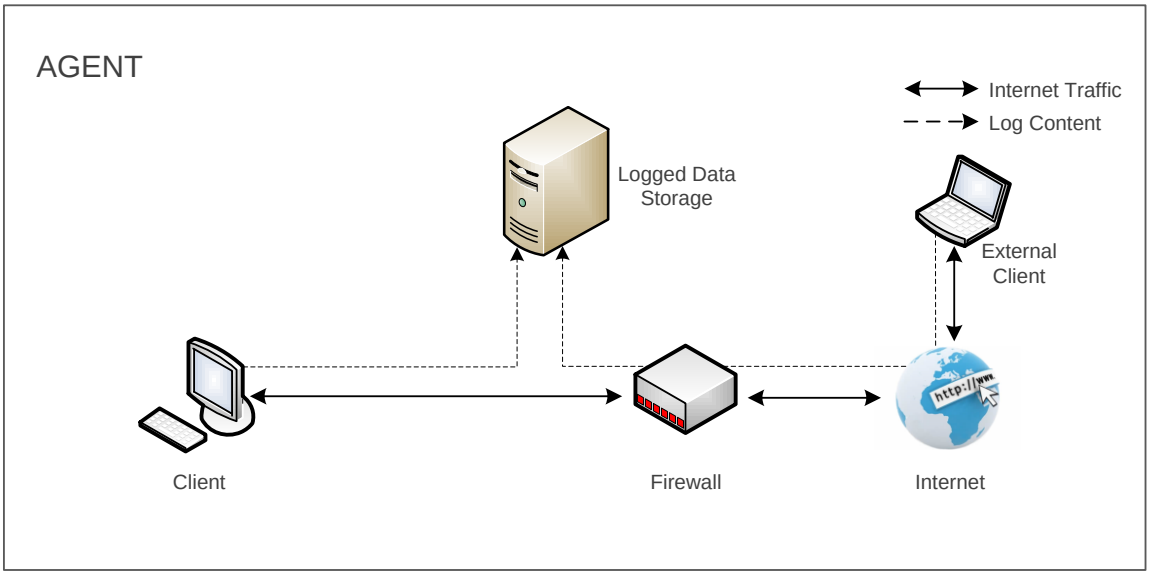
Pass-By



The Pass-By or network packet sniffer solution places a server or Internet appliance on selected subnets within the UIM environment. This architecture is based on the idea that all machines connected to a local network can see all the network traffic to and from all other machines on the same local network. As data streams travel back and forth over the network, the sniffer captures each packet, reassembles the stream based on the TCP/IP protocol and analyzes the content according to the appropriate application specification (e.g. SMTP protocol for email). Sniffers are used to analyze network problems, gather and report network statistics, spy on other network users to collect sensitive information like passwords, reverse engineer communication protocols used on the network and to monitor and control access to Internet content. The term "sniffer" originated from the first packet capture and decoding software that was offered for the purpose of network analysis and troubleshooting.

The placement of the sniffer is determined by the workstations to be monitored. In UIM operation, user Internet requests are monitored and analyzed as the request is being sent from the user to the desired Internet server. A decision about whether the server may be accessed is made at the sniffer server or appliance. If the content is determined to be off limits, the sniffer poses as the desired Internet server and sends an "access is denied" message back to the user. The returned information from the actual Internet server is then ignored by the user's application.

Client-Server



The Client-Server architecture places one or more servers in the UIM environment and installs a client program or Agent on each workstation in the UIM environment that is to be monitored and controlled. Each instance of the Agent can send requests to the server. In a Client-Server architecture, the server is usually passive, waiting for requests from the Agent - for example a list of allowable Internet access rules for the existing user or a request to receive and store captured data that describes the user's Internet activity. Upon receipt of requests, the server processes the request and then serves replies to the Agent. In a Client-Server architecture, the Agent is active, sending requests to the server and processing the replies received from the server. Client-Server architectures are commonly referred to as distributed architectures because the processing load is distributed to the clients. For example, the UIM agent may analyze a Web request at the client and make a decision whether or not to present data to the user based on Internet access rules it received from the server. The term Client-Server was first used in the 1980s in reference to PCs on a network. The Client-Server software architecture is a versatile, message-based and modular infrastructure that is intended to improve usability, flexibility, interoperability, and scalability as compared to centralized computing architectures.

In UIM operation, user requests to Internet content are monitored and analyzed locally in real-time by the Agent when the request is being sent to the desired Internet server. A decision about whether the content may be accessed is made at the user's workstation. If the transaction (Web site access, email content, IM payload) is determined to be off-limits, the Agent on the workstation prevents transmission of the request and immediately returns an access is denied message to the Internet application running on the machine.

Advantages and Disadvantages of the Solutions

Pass-Through

An advantage of the Pass-Through architecture is its single point of installation. This provides simple installation and reduced IT management. In most cases, Pass-Through architectures also provide proxy capability for Web access and thus improve Web access performance for the UIM environment. There are, however, a number of disadvantages to this architecture. The benefit of having a single point of installation also creates a potential single point of failure that must be addressed with redundancy. Since the UIM functionality in a Pass-Through environment requires all Web access to occur through a single point, the workstations in the UIM environment must be configured to direct Web access to the Pass-Through point or must be NAT'd to the Pass-Through point. It is therefore possible for a user to change their configuration or use alternate means to access the Web. This could include a readily available WiFi connection or a mobile modem. In addition, monitoring and controlling remote or mobile users that are not in the UIM environment requires the remote workstations to be directed back into the Pass-Through UIM environment, an inefficient and unreliable solution. Although somewhat offset by its caching capabilities, Pass-Through installations create a bottleneck to Internet content causing performance to suffer. In general, Pass-Through architectures are used only for Web and FTP activity monitoring and typically do not address other Internet communication protocols such as email, chat, IM and blog postings.

Pass-By

Advantages of the Pass-By architecture include potential single point of installation and the ability to monitor all types of network traffic. Deployment of a sniffer solution is straight forward on small networks but grows quickly in complexity in environments with multiple subnets. Since traffic is not visible to the sniffer computer across subnets, a sniffer computer must be installed on each subnet in a medium or large scale network. If a sniffer server or appliance fails, communication does not cease. This is typically the preferred failure mode except in highly secure implementations. A sniffer's inherent design makes Pass-By non-deterministic; sniffers must capture, analyze and control network traffic on the fly. Access to Internet content must be denied with an immediate response to the machine making the requests. It is quite possible in this type of architecture for the sniffer server or appliance to become overloaded and respond in a timeframe longer than the desired Internet server thus failing to reliably block prohibited content. As with the Pass-Through architecture, the Pass-By architecture also requires remote and mobile users to be inefficiently routed back through the UIM environment for each request for Internet content in order for the remote machine to be monitored and controlled. It is also possible to circumvent content monitoring and control by using a local WiFi connection or through the use of a mobile modem.

Client-Server

Advantages of the Client-Server architecture include scalability and limited processing requirements for the server. In addition, the Client-Server architecture provides real-time monitoring and control of remote and mobile users without re-routing communications through the local UIM environment. Because the UIM Agent is resident on the client, it is not possible to subvert the UIM solution by accessing the Internet through off-network means such as connection through WiFi hotspots or through modem connections. Circumvention is possible, however, by removing the Client-Server Agent from the client in non-secure implementations. As in the Pass-By architecture, a single point of failure will not impede the continuity of communications. By nature of its distributed design, the Client-Server implementation does not suffer from bottleneck performance issues found in the Pass-Through architecture nor does it suffer from processing overload typical in the Pass-By architecture. The disadvantages of this architecture relate to IT management issues. Agents must be deployed on all machines in the UIM environment. This can be time consuming for implementations that don't provide Agent management capabilities or situations where users don't authenticate on a network that administers the client's computer policies.

Summary

It is clear that each of the architectures described have a number of advantages and disadvantages. In an environment where workstations are well managed or mobile and/or remote office computing is present and consistent application of UIM rules is desired, the Client-Server architecture provides the most secure and robust solution. In cases where the configuration of the workstations is not controlled, users are stationary and bottle-neck issues are not a concern, the Pass-Thru or Pass-By solutions may be a suitable choice. Other considerations include the need to monitor various Internet protocols. In this situation, the Pass-By and Client-Server architectures are the most viable solutions.