Support Resources

TCS Basys Controls®

Firewall

Introduction

A firewall is intended to limit either access into a private network or out of it. A firewall can be built to prevent people from accessing inside your local network from the outside world. This is employed at TCS to prevent people on the Internet from accessing our computer systems and stealing our intellectual property. The other function is to limit Internet access to the users of your local network. A common scenario would be to prevent clerks in a retail environment from using the corporate WAN to surf the net and thus reducing productivity or clogging up the bandwidth.

There are two types of firewalls: packet filters and proxy servers. The packet filtering firewall looks at the individual packets (think addresses on your mail) and decides whether to allow it to pass through or not based on a set of rules. This is analogous to the function performed by the post office. It may check a list of valid addresses and send the letter back to the sender if it fails. With this function, you can create rules such that only let you use the HTTP protocol (the one your web browser uses) and deny people trying to use file sharing programs like Kazaa. The IT administrator may want to permit the retail stores to access the Internet, but to encourage productivity, only select sites are permitted so that the employees do not spend all of their bandwidth on espn.com. The firewall would then be configured to only permit certain sites through.

The second form of firewall is called a proxy server. When you try to access the Internet, you first tell the proxy server, and then it accesses the Internet for you and returns the results. For example, when you are trying to access CNN.com, your computer contacts the proxy server with the address you're requesting. The proxy server then goes out on the Internet and downloads the CNN.com home page. Finally, it returns the web page to your computer for display. A proxy server is commonly employed when there is no way to provide a direct connection to the Internet for each computer on a network. Additionally, because the proxy server does all the talking on the network, and it knows who requested what, it is very easy to log all the activity on the Internet. Commonly, a proxy server is configured as a web cache. Say a user just requested ebay.com, and now a second user has requested that page. The proxy server can use the stored version it got for the last user to satisfy the latest request for that web site. In this situation, only one request must be generated to the ebay.com server for the web page despite responding to two requests.

Application

When installing a firewall, common practice is to make it as restricting as possible and then open up ports or addresses as needed by the clients. This philosophy ensures that any unknown vulnerabilities in the network are protected by the firewall. This security measure ensures safety first at the risk of limiting the usefulness of the network given the restrictions. Then, as the system is used, and users needs increase, specific parts of the firewall can be opened for their use. For example, a QD2020 has specific requirements to contact the Ubiquity server. To permit that communication, the network administrator must open the firewall to permit the QD2020 to contact our Ubiquity URL (currently

216.165.178.150) using port 80 (the HTTP protocol). Thus, the IT contact would modify the configuration of the firewall to permit traffic from the QD2020's location on the local network to the Ubiquity URL.

If the firewall is constructed with a proxy server, care must be taken to ensure that the system does not cache the requests generated by the QD2020. When a QD2020 detects a change on its controller network, it uploads the information to the Ubiquity server and the server replies with an acknowledgment that it received the data. In a caching implementation, after the first request, the cache would intercept all subsequent requests to the Ubiquity server. From the QD2020s perspective, it keeps seeing the OK reply indicating the server successfully received its information. On the other end, the Ubiquity server would never hear any of the posted information since the web cache does not forward the data on and thus would be considered offline. Web caches often contain configuration parameters that prevent certain addresses from being cached and thus must be configured so for the Ubiquity URL.

APPENDIX A: QD2020 NETWORK PARAMETERS

To accommodate a QD2020 on a network, we have provided this list of network parameters. It entails an overview of the information necessary to configure a networking system to provide proper communication between the QD2020 and the Ubiquity server.

The QD2020 attempts a connection the Ubiquity server located at: *216.165.178.150, Port 80* Using the HTTP Protocol, the QD2020 first uploads any monitoring data using a POST command. The Ubiquity server responds with programming commands during the response from the same connection.

In the event that a connection cannot be established with the Ubiquity server, and a fallback alarm is detected, the QD2020 will attempt to open a connection with the programmed SMTP server (by default, this is set to tcsbasys.com, port 25).