

Task 4 - Access Control Lists

Now that you have configured our site to utilize Transport Layer Security (TLS), and greatly improved the security of our operations we have some additional concerns. We have noticed some unusual traffic directed to our **/admin** page. As this page can be used to manage, and configure our web site, we would like to restrict the access to this page. Our management group will require access to this page, and we have been informed they will utilize a machine with the IP 10.0.1.10 when they attempt to access the admin page. The local administrators on the machine hosting the server will also need access to preform routine checks.

The previous developers managing the site were absent minded at times, and may have pushed some unfinished or vulnerable pages to our repository. Feel free to block them if you do find them.

Again, the previous group did not produce the most comprehensive documentation when they were asked to look into this... We have recovered what we can and included it below for your convince.

Expected Outcome

1. Limit access to the **/admin** page
2. Allow the management group access
 - They are using a machine with an IP of 10.0.1.10
3. Allow the local administrator (using the machine hosting the site) access
4. Limit access to any unfinished or testing pages that are found

Old Documentations (DO NO IMPLEMENT)

Access Control Lists (ACL) are structures, that we use to define as set of rules. We use these rules to determine if the connection we are receiving is going to be accepted or rejected. This is of course based off of the conditions that we specify in the ACL.

In this case we are going to define a ACL as a operation done by the proxy. What proxy we are using is yet to be decided, but two common proxies are HAproxy and Nginx.

HAProxy is easier as we only need two (really three) lines to implement the Access Control List

```
# Limit access to those listed IPs
acl network_allowed src <ip1> <ip2>
# Limit access when a path begins with a specific line
acl restricted_page path_beg, url_dec -i /admin

# Block when above conditions are met (or in the case of network allowed not met)
block if restricted_page !network_allowed
```

If we need to implement it using Nginx, then the thinking is the same. However the exact implementation will be different.