Web Server Registration

Background

Web server registration is a low cost, low impact activity that has reasonable and specific benefits:

1. Reduced internet footprint - it is beneficial to reduce the Lab's exposure of unneeded and unmanaged web servers. Examples include printers and cameras, as well as misconfigured and abandoned web servers.
2. Awareness of openness to the Internet - web server owners specifically acknowledge the increased risk of opening their web server to the Internet. This acknowledgment will increase awareness of the risks, thus incentivizing properly securing exposed web servers.
3. Early security checkup - this process will allow Cyber to look for vulnerabilities before the web server is exposed to the Internet.

How To Register

1. To register a web server visit: [https://iprequest.lbl.gov/iprequest/portexceptions](https://iprequest.lbl.gov/iprequest/portexceptions)

2. Enter your computer name in the "Add, modify or remove a FQDN:" field and click "next".

3. Check the boxes next to the port exceptions you would like to create and click "next".

4. If you are done making changes, click "submit".

5. You will then receive an email like the one below that your request has been submitted.
6. The cyber security group is notified about your request. They will scan your web server for vulnerabilities. If no vulnerabilities are found the request will be approved. If vulnerabilities are found, you will be contacted to resolve them before the request is approved.

For urgent situations, where you need the web server immediately assessable please contact security@lbl.gov

How to Unregister (delete) a Web Server

1. To delete a web server visit: https://iprequest.lbl.gov/iprequest/portexceptions

2. Enter your computer name in the "Add, modify or remove a FQDN:" field and click "next".

3. Uncheck the boxes next to the port exceptions you would like to remove and click "next".

4. If you are done making changes, click "submit".

CPP Advisory:
For the vast majority of systems we recommend you use DHCP. DHCP gives your system more network flexibility than a static IP. You can reliably refer to your DHCP host by using [hostname]. dhcp.lbl.gov. The only reason you need to get a static IP address is if you intend to offer services beyond those listed below to the Internet.

https://commons.lbl.gov/x/k5R1B

By utilizing a fixed IP address, your system will be fully exposed to network traffic at the LBL Border. By requesting this address, you indicate that you understand the additional risks presented and that you will (as always) take appropriate precautions to secure your system.
5. You will then receive an email like the one below that your exception request is processing.

IP Request queue report

Miguel Salazar
to LBLnet, webserver-regi., CPP, Jay

Your request has been submitted.

Request:
#1 Delete port exceptions for kira.lbl.gov: 131.243.64.30 80/TCP, 443/TCP

Your will receive another email message when your request has been completed.

https://iprequest.lbl.gov/iprequest/

--------------------------

CPP Advisory:
For the vast majority of systems we recommend you use DHCP. DHCP gives your system more network flexibility than a static IP. You can reliably refer to your DHCP host by using [hostname].dhcp.lbl.gov. The only reason you need to get a static IP address is if you intend to offer services beyond those listed below to the Internet.

https://commons.lbl.gov/x/k5R1B

By utilizing a fixed IP address, your system will be fully exposed to network traffic at the LBL Border. By requesting this address, you indicate that you understand the additional risks presented and that you will (as always) take appropriate precautions to secure your system.

Email List for Registration

All registered web server contacts are added to the webserver-registration mailing list to announce vulnerabilities and communicate other important information. In order to join the webserver-registration mailing list you can use the form located here.

FAQ

1. How long after I make a registration request until it becomes accessible from the Internet?

   Our goal is less than 2 business days. We run multiple vulnerabilities scanners, which can take some time to run.

2. Can I register a DHCP host as a web server?

   No. In order to register a web server and have it be visible to the Internet, you must acquire a static IP address.

3. Why was my web server unregistered?
There are two reasons why the cyber security group will unregister a web server. The first is the web server is no longer online or no longer at the registered IP address. Unregistering the IP prevents some future computer at the IP from improperly becoming a registered web server without knowing it. The second reason is to protect the web server from some critical vulnerability as discussed here.

4. Do I need to register all the web servers virtual hosts and hostnames (i.e. cnames)?

The policy that enforces web server registration only understands IP addresses. Hence, web server registration is essentially IP based. If the computer has multiple named-based virtual hosts or cnames branched from one IP address, only the one IP address needs to register. If the host uses multiple IP addresses, one for each virtual host, all of the IP addresses need to be registered.

5. What if the IP address of my web server changes?

There is no way to change an IP address within the web server registration application. If the IP address of your web server changes, you will need to unregister the old web server IP and register the web server at the new IP address. For example, if your web server moves to a different building, it will likely get a new IP address.

6. Do I need to register 'HTTP' or 'HTTP and HTTPS'?

It depends. You may have to check with your server administrator or web programmer. The vast majority of web servers at the lab only have HTTP accesses from the Internet. If you are not sure, you can see if port 443/tcp is open on your web server. If the port is not open, it is unlikely you need HTTPS. CPP can help determine if you need HTTPS access, just let us know.

7. How can I confirm my web servers is registered?

a. Use onestop page at http://onestop.lbl.gov/onestop and examine the reported port exceptions.

<table>
<thead>
<tr>
<th>Report for kira.lbl.gov on Wednesday, October 14 2015 at 18:31:28 PDT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wired:</td>
</tr>
<tr>
<td>block: OK</td>
</tr>
<tr>
<td>syslog:</td>
</tr>
<tr>
<td>2015-10-14 18:21:54 permittcpdsthostport 131.243.64.30 <a href="mailto:iprequest@lns.lbl.gov">iprequest@lns.lbl.gov</a></td>
</tr>
<tr>
<td>2015-10-14 18:22:00 permittcpdsthostport 131.243.64.30 <a href="mailto:iprequest@lns.lbl.gov">iprequest@lns.lbl.gov</a></td>
</tr>
<tr>
<td>whitelist: NO</td>
</tr>
<tr>
<td>nullzero: OK</td>
</tr>
<tr>
<td>port exceptions: OK (443/TCP, 80/TCP)</td>
</tr>
</tbody>
</table>

8. What about Internet accessibility to other ports on my web server?

Web server registration does not affect any ports besides 80/tcp and 443/tcp. Internet accessibility to all other ports on your web server is unaffected by web server registration. For example, if you want to SSH (22/tcp) to your web server, that access remains unaffected whether or not your register your web server. Keep in mind CPP always recommends you configure your computer for minimum exposure to the Internet, while meeting your business needs.

9. What about web servers on non-standard ports?

We recognize that a web server can listen on any port, e.g. a non-standard port. Normally a web server listens on 80/tcp and a SSL enabled web server listens on port 443/tcp. The case where web servers run on non-standard ports is not addressed by web server registration at this time. If you would like to run a web server on a non-standard port, no registration is required. The cost-benefit-calculus for registering web servers on non-standard ports or requiring web servers to use standard ports is not clear.

10. I need to run some other application, that is not a web server, on 80/tcp or 443/tcp. Do I need to register?

Yes. If you have some device or application that is not a web server and needs 80/tcp or 443/tcp to be visible from the Internet, it must be registered. For example, if you have a web camera that you control from the Internet via 443/tcp, the camera needs to be registered.

11. Are registered web servers open to the entire Internet?

Not necessarily. Registration allows traffic to reach a web server through the LBNL border router, but host or local firewalls may further restrict access. CPP recommends and encourages web servers be configured to restrict traffic to the minimum required, commonly
referred to as the principle of least privilege. For example, if your web server only needs to be accessed from NERSC, implement local firewall rules that only allow access from NERSC.

12. How do I update my web server contacts?

Web server contacts can be updated through https://iprequest.lbl.gov/iprequest. Once logged in, enter your computer name and click next. The next page has a field that contains “Modify contacts or location” in its title.

Policy

Web servers and applications must be fully configured and production-ready before a vulnerability scan is requested. Registration requests for web servers which are improperly or incompletely configured, or applications not running final production code, may be denied to avoid inaccurate or premature scan results.

Web servers may be automatically un-registered by Cyber Security if they meet any of following conditions:

1. Web servers flagged with a significant vulnerability
2. Web server not on the network for 30 days (arp data)
3. Web server has no network traffic from the Internet in last 30 days
4. Web server not enabled (listening) in last 30 days

Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Traffic</td>
<td>Network traffic on tcp port 80 or tcp port 443.</td>
</tr>
<tr>
<td>Web Server</td>
<td>Any device that accepts web traffic, that is, that listens on tcp port 80, normally for the HTTP protocol, or tcp port 443, normally for HTTPS protocol.</td>
</tr>
<tr>
<td>Internet</td>
<td>Any address space outside of 131.243.* and 128.3.*.</td>
</tr>
<tr>
<td>Intranet</td>
<td>the address space within 131.243.* and 128.3.*.</td>
</tr>
<tr>
<td>Berkeley Lab network</td>
<td>Synonymous with intranet.</td>
</tr>
</tbody>
</table>

¹ Internet here includes the address space of organizations closely affiliated with Berkeley Lab, such as NERSC, ESnet, JGI, and others.

Help/Feedback

If you have questions or comments about this website, please contact the CPP group via email at security@lbl.gov.

If you need general computer assistance, please contact the LBNL Help Desk at x4357, help@lbl.gov, or online at http://help.lbl.gov.