# DMZ Lab

This lab was developed for the Labtainer framework by the Naval Postgraduate School, Center for Cybersecurity and Cyber Operations under National Science Foundation Award No. 1438893. This work is in the public domain, and cannot be copyrighted.

## 1 Overview

This lab requires that you configure a DMZ using iptables on two gateway components.

## 2 Lab Environment

This lab runs in the Labtainer framework, available at http://my.nps.edu/web/c3o/labtainers. That site includes links to a pre-built virtual machine that has Labtainers installed, however Labtainers can be run on any Linux host that supports Docker containers.

From your labtainer-student directory start the lab using:

```
labtainer dmz-lab
```

A link to this lab manual will be displayed.

## 3 Network Configuration

This lab includes several networked computers as shown in Figure **??**. Note however that your instance of the lab will have different IP addresses for some of the components. When the lab starts, you will get several virtual terminals, one connected to each component.

The outer gateway and the remote gateway each reach the Internet via an ISP with address 198.18.0.1. The local site has a network address of 198.18.1.0/24. The remote site has a network address of 203.0.113.0/24.

Initially, the DMZ is in name only.

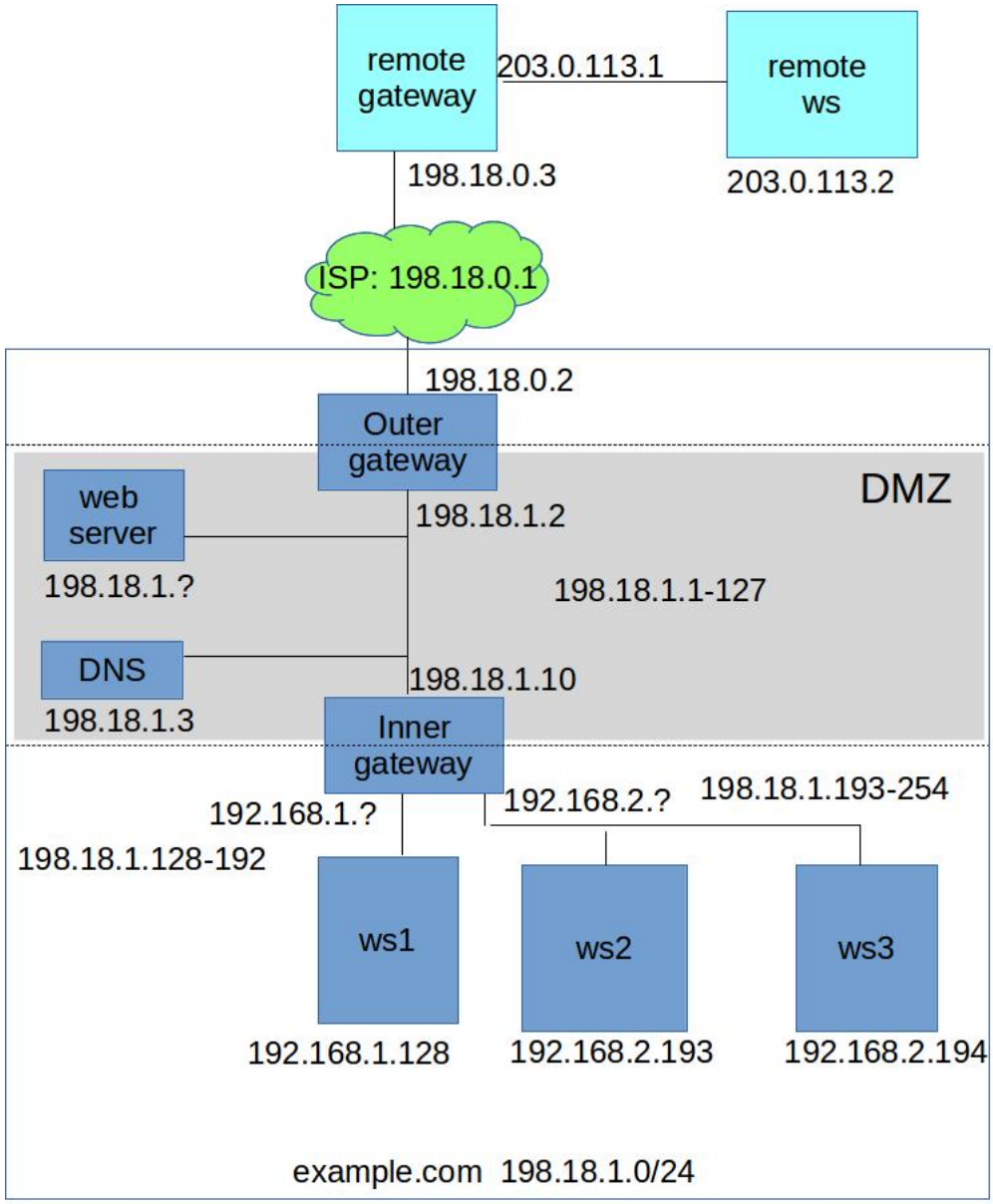


Figure 1: Network topology for dmz-lab

## 4 Lab Tasks

Configure the inner_gateway and outer_gateway such that:

- Remote users can only access the web server, e.g., via wget www.example.com, using HTTP, HTTPS and SSH.
- Local users can reach the internet via the ISP, e.g., wget www.google.com
- Local users can reach the local web server via HTTP, HTTPS, SSH and MYSQL

Use the /etc/rc.local scripts on the inner and outer gateways to issue iptables directives. Respect the comments in the rc.local scripts regarding sections that should not be modified. Demonstrate your DMZ by issuing the following commands, without any additional changes to iptables.

1. On the remote_ws (hank): `sudo nmap www.example.com`
2. On the ws1 (tom): `sudo nmap www.example.com`
3. On the ws1 (tom): `wget www.google.com`

If you make any changes to iptables in the course of your testing, restart your testing from item (1) above.

# 5 Submission

After finishing the lab, go to the terminal on your Linux system that was used to start the lab and type:

```
stoplab dmz-lab
```

When you stop the lab, the system will display a path to the zipped lab results on your Linux system. Provide that file to your instructor, e.g., via the Sakai site.