* [Class 3: ASM 141 - Good WAF Security, Getting started with ASM](https://clouddocs.f5.com/training/community/waf/html/class3/class3.html)
* [Class 4: ASM 241 - Elevating ASM Protection](https://clouddocs.f5.com/training/community/waf/html/class4/class4.html)
* [Class 5: ASM 341 - High and Maximum Security](https://clouddocs.f5.com/training/community/waf/html/class5/class5.html)
* [Class 6: ASM 342 - WAF Programmability](https://clouddocs.f5.com/training/community/waf/html/class6/class6.html)
* [Class 7: API Protection with ASM](https://clouddocs.f5.com/training/community/waf/html/class7/class7.html)
* [Class 3: ASM 141 - Good WAF Security, Getting started with ASM](https://clouddocs.f5.com/training/community/waf/html/class3/class3.html)

**Lab Environment & Topology**[**¶**](https://clouddocs.f5.com/training/community/waf/html/class3/labinfo/labinfo.html#lab-environment-topology)

Note

All work is done from the Linux client/jumphost (client01), which can be accessed via RDP (Windows Remote Desktop) or ssh. No installation or interaction with your local system is required.

**Environment**[**¶**](https://clouddocs.f5.com/training/community/waf/html/class3/labinfo/labinfo.html#environment)

**Linux client (client01):**

**Web Attack Tools used in this lab:**

* [OWASP ZAP](https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project) - DAST
* [BURP Community Edition](https://portswigger.net/burp/) - Packet Crafting

**Api Tools:**

* [Ansible](https://www.ansible.com/) - Automation platform
* [curl](https://curl.haxx.se/) - command line webclient, will be used to interact with the iControl Rest API
* [Postman](https://www.getpostman.com/) - Graphical based Restful Client, will be used to interact with the iControl Rest API
* [python](https://www.python.org/) - general programming language used to interact with the iControl Rest API

**Linux server (server01):**

* [WebGoat 8](https://github.com/WebGoat/WebGoat/wiki) - WebGoat is a deliberately insecure web application maintained by OWASP designed to teach web application security lessons.

**Lab Topology**[**¶**](https://clouddocs.f5.com/training/community/waf/html/class3/labinfo/labinfo.html#lab-topology)

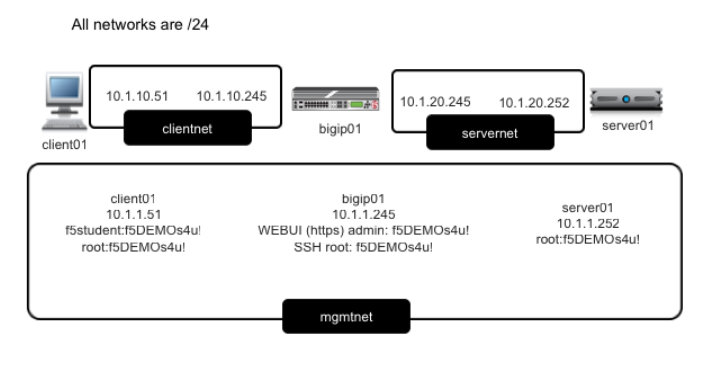
The network topology implemented for this lab is very simple. The following components have been included in your lab environment:

* 1 x Ubuntu Linux 16.04 client
* 1 x F5 BIG-IP VE (v13.1.0.2) running ASM and LTM
* 1 x Ubuntu Linux 16.04 server

The following table lists VLANS, IP Addresses and Credentials for all components:

| **COMPONENT** | **MGMTNET IP** | **CLIENTNET IP** | **SERVERNET IP** | **CREDENTIALS** |
| --- | --- | --- | --- | --- |
| Linux Client (client01) | 10.1.1.51 | 10.1.10.51 | N/A | https-ubuntu:ubuntu |
| Bigip (bigip01) | 10.1.1.245 | 10.1.10.245 | 10.1.20.245 | https - admin:f5DEMOs4u!ssh - f5student:f5DEMOs4u! |
| Linux Server & WebGOAT app (server01) | 10.1.1.252 | N/A | 10.1.20.252 | ssh - f5student:f5DEMOs4u! |

A graphical representation of the lab:



* webgoat.f5demo.com\_https\_vs
* webgoat.f5demo.com\_https\_overlay\_vs
* webgoat.f5demo.com\_http\_vs : 10.1.10.145:443
* automation\_vs

