Create a set of firewall rules that provide a reasonable amount of security to the internal network. Make sure you address the rules mentioned by the client above, as well as these extra requirements:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Action(Drop/Reject)** | **In/Out** | **SRC** | **DEST** | **PROTO** | **PORT** |
| 1 | Drop | In | ANY | ANY | ICMP | \* |
| 2 | Reject | In | ANY | 172.16.3.1 | TCP | 3306 |
| 3 | Drop | Out | 192.158.1.38 | ANY | TCP | 22 |
| 4 | Drop | Out | 172.16.9.1 | ANY | TCP | 22 |
| 5 | Reject | In | ANY | 172.16.4.1 | TCP | \* |
| 6 | Allow | In | 189.61.4.203 | 172.16.3.1 | TCP | 3306 |
| 7 | Allow | In | 101.99.230.16 | 172.16.3.1 | TCP | 3306 |
| 8 | Reject | In | ANY | 172.16.2.1 | ANY | \* |
| 9 | Reject | In | ANY | 172.16.6.0/24 | ANY | \* |
| 10 | Reject | In | ANY | ANY | TCP | 21 |
| 11 | Reject | In | ANY | ANY | TCP | 20 |

1. Do not respond to ping requests.
2. Reject MySQL requests from the Internet. (database server)
3. Drop all ssh traffic outbound from the web server.
4. Reject any source from the internet to payroll server.
5. Reject any source from the web server.
6. 189.61.4.203 allow for client.
7. 101.99.230.16 allow for client.
8. Security camera reject any from internet.
9. Reject any Industrial Machine.
10. Reject any FTP
11. Reject any FTP