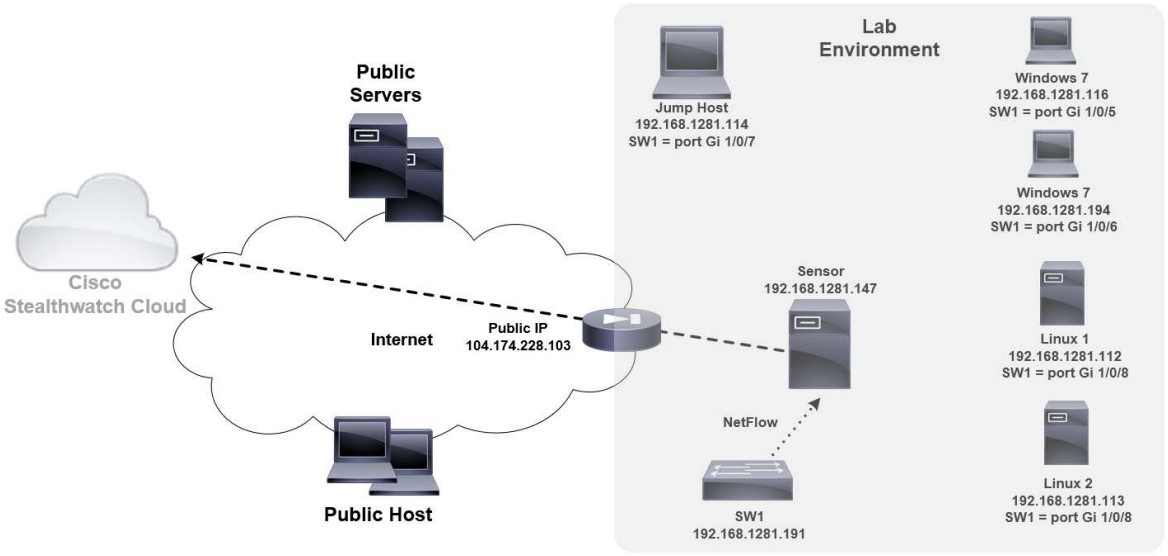
Project Summary

1) Communication between the Windows and Linux machines will be reported through NetFlow.

Project Details

To be determined.



Note: traffic between Linux1 and Linux2 will not trigger Netflow because they are on the same port and will not pass through SW1.

Access Information

Windows .116 – username: admin / Password: WWTwwt1!
Windows .194 – username: admin / Password: WWTwwt1!
Linux 1 – username: root / Password: WWTwwt1!
Linux 2 – username: root / Password: WWTwwt1!
Switch SSH – username: admin / Password: WWTwwt1!
Switch – enable password: WWTwwt1!
Sensor – username: administrator / Password: WWTwwt1!

NetFlow Configuration on SW1

```
!
flow record Netflow-In
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface input
 match flow direction
 match flow cts source group-tag
 match flow cts destination group-tag
 collect interface output
 collect counter bytes long
 collect counter packets long
 collect counter bytes layer2 long
```

```
!
!
flow record Netflow-Out
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface output
 match flow direction
 match flow cts source group-tag
 match flow cts destination group-tag
 collect interface input
 collect counter bytes long
 collect counter packets long
 collect counter bytes layer2 long
!
flow exporter Netflow-to-SW
 description Export NetFlow to StealthWatch
 destination 192.168.128.147         <<<<<<<<<<< Sensor Address
 source Vlan1
 transport udp 2055
!
flow monitor Netflow-Monitor-In
 exporter Netflow-to-SW
 cache timeout inactive 10
 cache timeout active 60
 record Netflow-In
!
flow monitor Netflow-Monitor-Out
 exporter Netflow-to-SW
 cache timeout inactive 10
 cache timeout active 60
 record Netflow-Out
!
interface GigabitEthernet1/0/5
 ip flow monitor Netflow-Monitor-In input
 ip flow monitor Netflow-Monitor-Out output
!
interface GigabitEthernet1/0/6
 ip flow monitor Netflow-Monitor-In input
 ip flow monitor Netflow-Monitor-Out output
!
interface GigabitEthernet1/0/7
 ip flow monitor Netflow-Monitor-In input
 ip flow monitor Netflow-Monitor-Out output
!
interface GigabitEthernet1/0/8
 ip flow monitor Netflow-Monitor-In input
 ip flow monitor Netflow-Monitor-Out output
!
interface Vlan1
 ip address 192.168.128.191 255.255.255.0
!
```