# Docker Swarm Mode Ports
Starting with 1.12 in July 2016, Docker *Swarm Mode* is a built-in solution with built-in key/value store. Easier to get started, and fewer ports to configure.

## Inbound Traffic for Swarm Management
- TCP port 2377 for cluster management & raft sync communications
- TCP and UDP port 7946 for "control plane" gossip discovery communication between all nodes
- UDP port 4789 for "data plane" VXLAN overlay network traffic
- IP Protocol 50 (ESP) if you plan on using overlay network with the encryption option

## AWS Security Group Example
AWS Tip: You should use Security Groups in AWS's "source" field rather then subnets, so SG's will all dynamically update when new nodes are added.

### Inbound to Swarm Managers (superset of worker ports)
Type	Protocol	Ports	Source
Custom TCP Rule	TCP	2377	swarm + remote mgmt
Custom TCP Rule	TCP	7946	swarm
Custom UDP Rule	UDP	7946	swarm
Custom UDP Rule	UDP	4789	swarm
Custom Protocol	50	all	swarm

### Inbound to Swarm Workers
Type	Protocol	Ports	Source
Custom TCP Rule	TCP	7946	swarm
Custom UDP Rule	UDP	7946	swarm
Custom UDP Rule	UDP	4789	swarm
Custom Protocol	50	all	swarm

# Docker Swarm "Classic" Ports, with Consul
For Docker 1.11 and older. I Used [this list from Docker Docs on Swarm Classic](https://docs.docker.com/swarm/plan-for-production/#/network-access-control), then tested on multiple swarms.

### Inbound to Swarm Nodes
 - 2375 TCP for swarm manger -> nodes (LOCK PORT DOWN, no auth)
 - 7946 TCP/UDP for container network discovery from other swarm nodes

 - 4789 UDP container overlay network from other swarm nodes

### Inbound to Swarm Managers
 - 3375 TCP for spawner -> swarm manager (LOCK PORT DOWN, no auth)

### Inbound to Consul
 - 8500 TCP for swarm manager/nodes -> consul server (LOCK PORT DOWN, no auth)
 - 8300 TCP for consul agent -> consul server
 - 8301 TCP/UDP for consul agent -> consul agent
 - 8302 TCP/UDP for consul server -> consul server

## Swarm Classic Inbound Ports In AWS Security Group Format, with Consul

AWS Tip: You should use Security Groups in AWS's "source" field rather then subnets, so SG's will all dynamically update when new nodes are added.

This is another way to look at the above lists, in a format that makes sense for AWS SG's
 - assume AWS inbound from:
   - Internet ELB -> Swarm Managers
   - Swarm Managers -> Swarm Nodes
   - Swarm Managers -> Consul Internal ELB
   - Swarm Nodes -> Consul Internal ELB
   - Consul Internal ELB -> Consul Nodes

### ELB Swarm Manager
Type	Protocol	Ports	Source
Custom TCP Rule	TCP	3375	spawners

### Swarm Managers
Type	Protocol	Ports	Source
Custom TCP Rule	TCP	3375	elb-swarm-manager

### Swarm Nodes
Type	Protocol	Ports	Source
Custom TCP Rule	TCP	2375	swarm-managers
Custom TCP Rule	TCP	7946	swarm-nodes
Custom UDP Rule	UDP	7946	swarm-nodes
Custom UDP Rule	UDP	4789	swarm-nodes

### ELB Consul
Type	Protocol	Ports	Source
Custom TCP Rule	TCP	8500	swarm-nodes
Custom TCP Rule	TCP	8500	swarm-managers

### Consul Nodes
Type	Protocol	Ports	Source
Custom TCP Rule	TCP	8500	elb-consul
Custom TCP Rule	TCP	8300-8302	consul-nodes
Custom UDP Rule	UDP	8301-8302	consul-nodes