Baseline AWS Network ACL

- Important IPs and CIDR Blocks
- CloudFormation
- Terraform
- Manual Configuration
  - Inbound Rules
  - Outbound Rules

This network ACL is the recommended baseline for VPC subnets in Cornell AWS accounts. It should be configured and used on all AWS VPC subnets. You are welcome to make your NACL more stringent, but we recommend careful consideration before making it less stringent.

Important IPs and CIDR Blocks

These IPs and CIDR blocks are referenced in the Baseline NACL:

CIDR	DNS Name	Description
52.200.35.38/32	kerberos-aws.login.cornell.edu	AWS-based Cornell Kerberos Server
52.201.66.104/32	kerberos-aws2.login.cornell.edu	AWS-based Cornell Kerberos Server
10.0.0.0/8		Cornell private network
128.84.0.0/16		Cornell campus public IPs
128.253.0.0/16		Cornell campus public IPs
132.236.0.0/16		Cornell campus public IPs
192.35.82.0/24		Cornell campus public IPs
192.122.235.0/24		Cornell campus public IPs
192.122.236.0/24		Cornell campus public IPs
35.170.14.255/32	test.directory.cornell.edu	AWS-based TEST directory
3.229.3.150/32	test.directory.cornell.edu	AWS-based TEST directory
3.228.209.25/32	query.directory.cornell.edu	AWS-based PROD directory
3.218.140.210/32	query.directory.cornell.edu	AWS-based PROD directory
100.64.0.0/10		AWS VPCs can be extended with CIDR blocks in this range.

> If you have extended your VPC using CIDR blocks from the 100.64.0.0/10 range, you will need to request a NACL rule quote increase. The default limit for NACL rules is 20. The outbound rule list for the baseline NACL is already 20 rules, not including any rules for 100.64.0.0/10 blocks. You will need to request a quota increase to at least 21 to accommodate a 100.64.0.0/10 rule. See VPC Network ACL quotas in AWS documentation.

CloudFormation

A CloudFormation template to create a Network ACL for with the baseline rules can be found here: https://github.com/CU-CommunityApps/cu-aws-cloudformation/tree/master/baseline-nacl

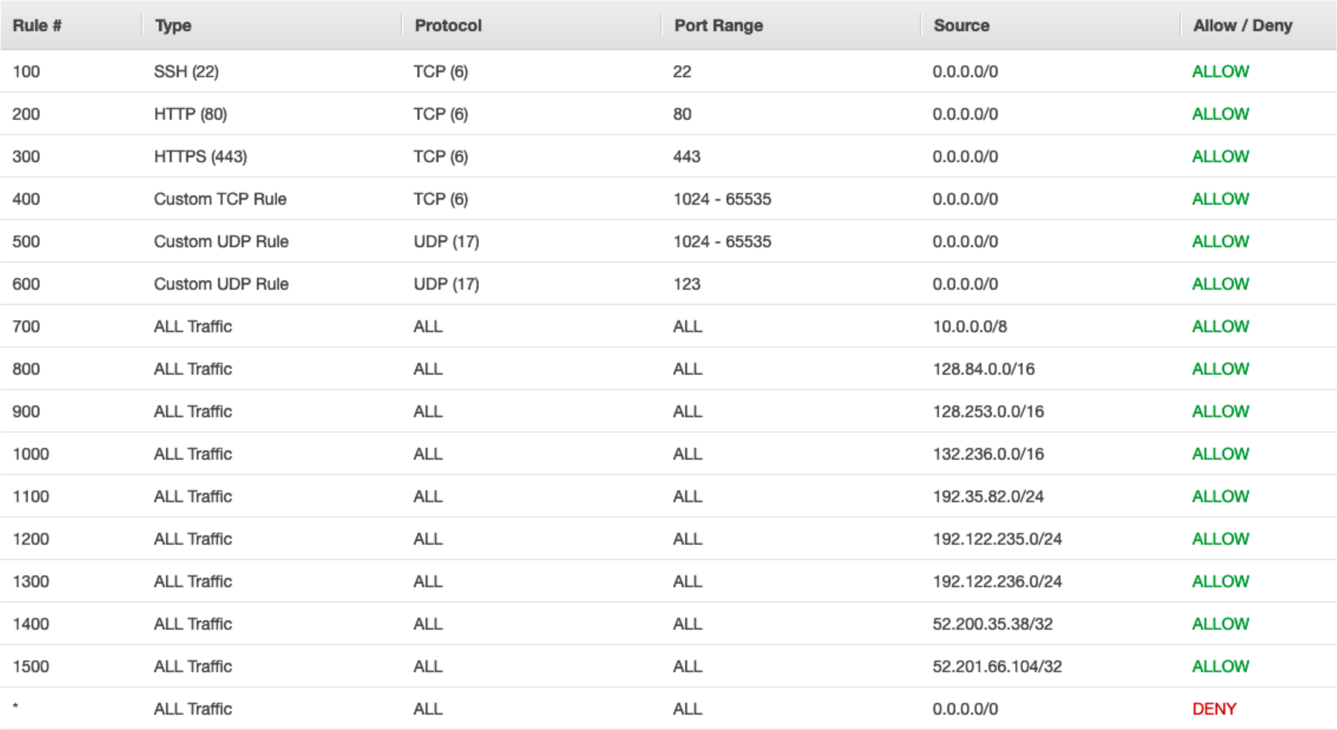
Terraform

A Terraform module to create a Network ACL with these baseline rules can be found here: https://github.com/CU-CommunityApps/tf-module-cornell-util/tree/main/modules/aws/baseline-nacl

Manual Configuration

Inbound Rules

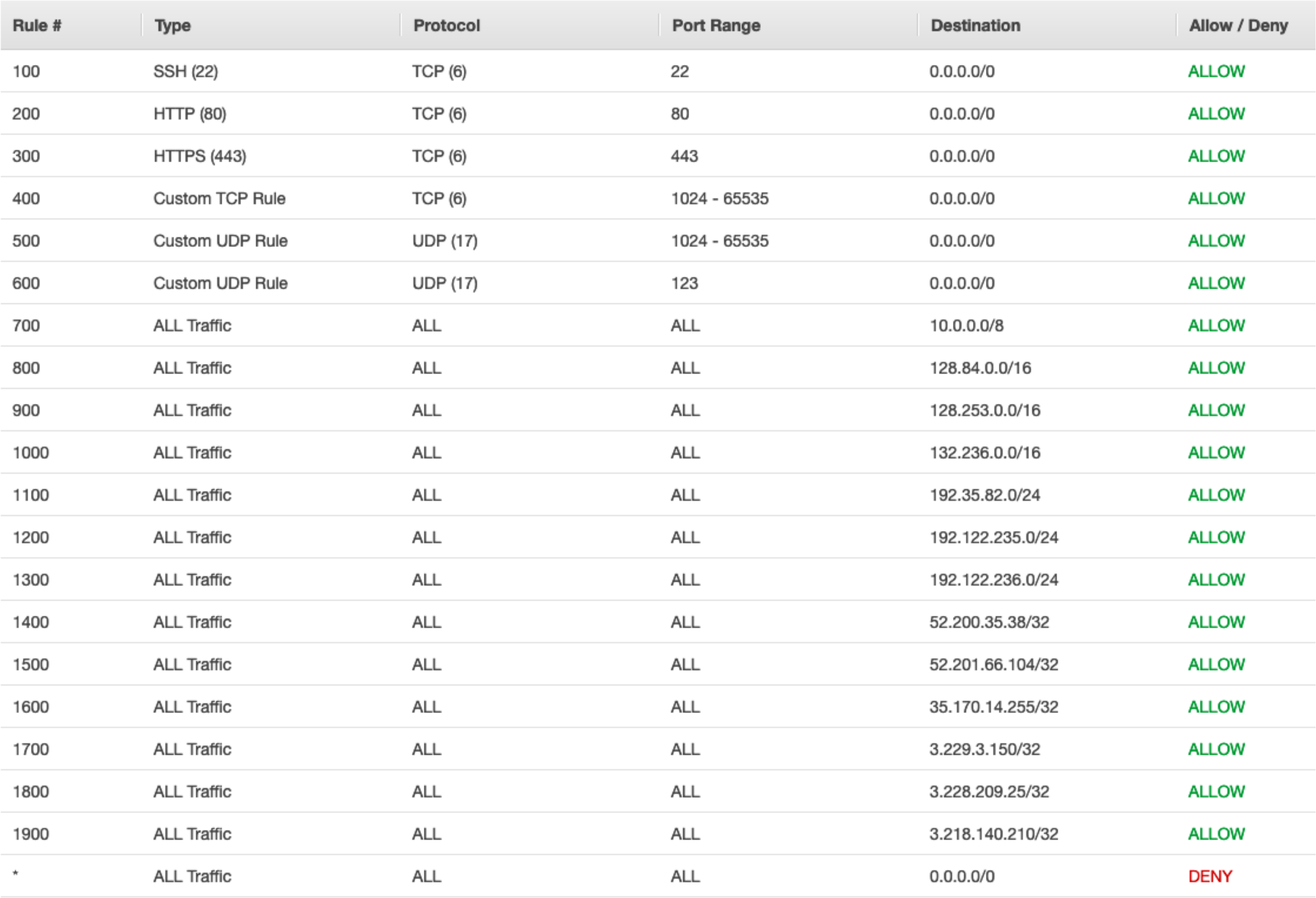
⚠️ Add an additional **ALLOW** rule **1600** to allow all traffic from source 100.64.0.0/10 if your VPC includes any CIDR blocks in 100.64.0.0/10.



Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	SSH (22)	TCP (6)	22	0.0.0.0/0	ALLOW
200	HTTP (80)	TCP (6)	80	0.0.0.0/0	ALLOW
300	HTTPS (443)	TCP (6)	443	0.0.0.0/0	ALLOW
400	Custom TCP Rule	TCP (6)	1024 - 65535	0.0.0.0/0	ALLOW
500	Custom UDP Rule	UDP (17)	1024 - 65535	0.0.0.0/0	ALLOW
600	Custom UDP Rule	UDP (17)	123	0.0.0.0/0	ALLOW
700	ALL Traffic	ALL	ALL	10.0.0.0/8	ALLOW
800	ALL Traffic	ALL	ALL	128.84.0.0/16	ALLOW
900	ALL Traffic	ALL	ALL	128.253.0.0/16	ALLOW
1000	ALL Traffic	ALL	ALL	132.236.0.0/16	ALLOW
1100	ALL Traffic	ALL	ALL	192.35.82.0/24	ALLOW
1200	ALL Traffic	ALL	ALL	192.122.235.0/24	ALLOW
1300	ALL Traffic	ALL	ALL	192.122.236.0/24	ALLOW
1400	ALL Traffic	ALL	ALL	52.200.35.38/32	ALLOW
1500	ALL Traffic	ALL	ALL	52.201.66.104/32	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Outbound Rules

⚠️ Add an additional **ALLOW** rule **2000** to allow all traffic to destination 100.64.0.0/10 if your VPC includes any CIDR blocks in 100.64.0.0/10.



Rule #	Type	Protocol	Port Range	Destination	Allow / Deny
100	SSH (22)	TCP (6)	22	0.0.0.0/0	ALLOW
200	HTTP (80)	TCP (6)	80	0.0.0.0/0	ALLOW
300	HTTPS (443)	TCP (6)	443	0.0.0.0/0	ALLOW
400	Custom TCP Rule	TCP (6)	1024 - 65535	0.0.0.0/0	ALLOW
500	Custom UDP Rule	UDP (17)	1024 - 65535	0.0.0.0/0	ALLOW
600	Custom UDP Rule	UDP (17)	123	0.0.0.0/0	ALLOW
700	ALL Traffic	ALL	ALL	10.0.0.0/8	ALLOW
800	ALL Traffic	ALL	ALL	128.84.0.0/16	ALLOW
900	ALL Traffic	ALL	ALL	128.253.0.0/16	ALLOW
1000	ALL Traffic	ALL	ALL	132.236.0.0/16	ALLOW
1100	ALL Traffic	ALL	ALL	192.35.82.0/24	ALLOW
1200	ALL Traffic	ALL	ALL	192.122.235.0/24	ALLOW
1300	ALL Traffic	ALL	ALL	192.122.236.0/24	ALLOW
1400	ALL Traffic	ALL	ALL	52.200.35.38/32	ALLOW
1500	ALL Traffic	ALL	ALL	52.201.66.104/32	ALLOW
1600	ALL Traffic	ALL	ALL	35.170.14.255/32	ALLOW
1700	ALL Traffic	ALL	ALL	3.229.3.150/32	ALLOW
1800	ALL Traffic	ALL	ALL	3.228.209.25/32	ALLOW
1900	ALL Traffic	ALL	ALL	3.218.140.210/32	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY