Edge protection deployment checklist

TIP: Only write the first four or five digits of the ID numbers, enough to differentiate the IDs. Write the complete CIDR addresses.

Create VPCs, subnets, and gateways

VPC ID:	vpc-	**VPC IPv4 CIDR:**	
Inspection subnet ID:	subnet-	**Inspection subnet IPv4 CIDR:**	
Management subnet ID:	subnet-	**Management subnet IPv4 CIDR:**	
Protected-public subnet ID:	subnet-	**Protected-public subnet IPv4 CIDR:**	
Protected-private subnet ID:	subnet-	**Protected-private subnet IPv4 CIDR:**	
Internet Gateway ID:	igw-	**NAT Gateway ID:**	nat-
Virtual Private Gateway ID:		**ON PREM CIDRs**	

Create security groups

Management security group ID:	sg-	**Traffic security group ID:**	sg-

Create an IAM policy

Policy name:	CloudWatch_logs_policy	**Role name:**	CloudWatch_logs

Create Network Protection instance

SSH key:		**Network Protection instance ID:**	i-

Create Elastic Network Interfaces

Port 1A (eth1) ID:	eni-	**Port 1A (eth1) IPv4 Private IP:**	
Port 1B (eth2) ID:	eni-	**Port 1B (eth2) IPv4 Private IP:**	

Make additional Network Protection configurations

SMS API key:		**SMS IP address:**	

AWS Cloud

Inspection VPC

Inspection subnet

<VPC CIDR>	Local	172.16.0.0 172.16.1.0 172.16.2.0
0.0.0.0/0	Internet Gateway	

Management subnet

<VPC CIDR>	Local	172.16.0.0 172.16.1.0 172.16.2.0
0.0.0.0/0	eni-1B	

eni-1A   management

Network Protection

eni-1B

Internet Gateway

<VPC CIDR>	Local	172.16.0.0 172.16.1.0 172.16.2.0
<management subnet>	eni-1A	
<protected-public subnet>	eni-1A	

Protected-public subnet

<VPC CIDR>	Local	172.16.0.0 172.16.1.0 172.16.2.0
0.0.0.0/0	eni-1B	

NAT gateway   Elastic Load Balancing   Public Instances

Protected-private subnet

<VPC CIDR>	Local	172.16.0.0 172.16.1.0 172.16.2.0
0.0.0.0/0	NAT Gateway	

Private Instances