**Cloud Architect interview by Mike Gibbs**

1. **What is a man in the middle attack?**

This is basically when there is a snicky IC in the middle of your conversation between A and B.

1. **How do you prevent a man in the middle attack?**

To do some end-point verification by using some form of encryption.. you can use WPA or WEP for wireless network.

1. **What is data protection when talking about encryption in transit vs encryption in rest?**

This is encrypting the data stored in the hard drive. Encryption protocols include VPN, IPSEC etc.

1. **What is the difference between symmetric and asymmetric encryption?**

Symmetric encryption is when you use the same encryption key to send and receive your data traffic while asymmetric encryption is when you use two different encryption keys to send and receive data.

1. **What is NMAP?**

This is a network map and it is a free open source tool that will help you find the hosts that are available, open ports on your systems, security risks and help hack into a system by white hackers or ethical hacking.

1. **What is IAM?**

This is identification of the users that have access to your systems, authorizing them to do things that are related to their roles and locking what they did so you can track what activities they did. This is also known as the concept of TRIPLE A which stands for Authentication, Authorization and Accountability. Authentication is making sure the user is the user, Authorization is determining what the user is allowed to do on the network and letting them do their role on the system and Accountability is tracking them.

1. **What is social engineering?**

This is the use of deception to get information from people. This is pretending to be somebody.

1. **How would you secure an enterprise?**
2. First you start with the policy and the policy would describe what type of device your protecting and so on. You also need to consider the user perspective, encryption perspective, IAM perspective and Tech perspective. First you build a firewall in your organisation, then the IDS or IPS systems which is Intrusion Detection and Intrusion Prevention systems which they add a new firewall rule. Next, you need some DDoS protection and that is your cloudfare or AWS Shield which are some type of DNS protection to prevent this attack. Then protecting your routers with network ACLs, you need to implement security groups for your host network, you also need to train your staff to avoid phishing or social engineering.

AWS: Allows access based on date and time

[**PDF**](https://docs.aws.amazon.com/pdfs/IAM/latest/UserGuide/iam-ug.pdf#reference_policies_examples_aws-dates)[**RSS**](https://docs.aws.amazon.com/IAM/latest/UserGuide/aws-iam-release-notes.rss)

This example shows how you might create an identity-based policy that allows access to actions based on date and time. This policy restricts access to actions that occur between April 1, 2020 and June 30, 2020 (UTC), inclusive. This policy grants the permissions necessary to complete this action programmatically from the AWS API or AWS CLI. To use this policy, replace the *italicized placeholder text* in the example policy with your own information. Then, follow the directions in [create a policy](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_create.html) or [edit a policy](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_manage-edit.html).

To learn about using multiple conditions within the Condition block of an IAM policy, see [Multiple values in a condition](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_condition.html#Condition-multiple-conditions).

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Action": "*service-prefix*:*action-name*",

"Resource": "\*",

"Condition": {

"DateGreaterThan": {"aws:CurrentTime": "2020-04-01T00:00:00Z"},

"DateLessThan": {"aws:CurrentTime": "2020-06-30T23:59:59Z"}

}

}

]

}

Enable or disable aws regions

{

"Version": "2012-10-17",

"Statement": [

{

"Sid": "EnableDisableHongKong",

"Effect": "Allow",

"Action": [

"account:EnableRegion",

"account:DisableRegion"

],

"Resource": "\*",

"Condition": {

"StringEquals": {"account:TargetRegion": "*ap-east-1*"}

}

},

{

"Sid": "ViewConsole",

"Effect": "Allow",

"Action": [

"aws-portal:ViewAccount",

"account:ListRegions"

],

"Resource": "\*"

}

]

}

{

"Version": "2012-10-17",

"Statement": [

{

"Sid": "AllowViewAccountInfo",

"Effect": "Allow",

"Action": [

"iam:GetAccountPasswordPolicy",

"iam:ListVirtualMFADevices"

],

"Resource": "\*"

},

{

"Sid": "AllowManageOwnPasswords",

"Effect": "Allow",

"Action": [

"iam:ChangePassword",

"iam:GetUser"

],

"Resource": "arn:aws:iam::\*:user/${aws:username}"

},

{

"Sid": "AllowManageOwnAccessKeys",

"Effect": "Allow",

"Action": [

"iam:CreateAccessKey",

"iam:DeleteAccessKey",

"iam:ListAccessKeys",

"iam:UpdateAccessKey"

],

"Resource": "arn:aws:iam::\*:user/${aws:username}"

},

{

"Sid": "AllowManageOwnSigningCertificates",

"Effect": "Allow",

"Action": [

"iam:DeleteSigningCertificate",

"iam:ListSigningCertificates",

"iam:UpdateSigningCertificate",

"iam:UploadSigningCertificate"

],

"Resource": "arn:aws:iam::\*:user/${aws:username}"

},

{

"Sid": "AllowManageOwnSSHPublicKeys",

"Effect": "Allow",

"Action": [

"iam:DeleteSSHPublicKey",

"iam:GetSSHPublicKey",

"iam:ListSSHPublicKeys",

"iam:UpdateSSHPublicKey",

"iam:UploadSSHPublicKey"

],

"Resource": "arn:aws:iam::\*:user/${aws:username}"

},

{

"Sid": "AllowManageOwnGitCredentials",

"Effect": "Allow",

"Action": [

"iam:CreateServiceSpecificCredential",

"iam:DeleteServiceSpecificCredential",

"iam:ListServiceSpecificCredentials",

"iam:ResetServiceSpecificCredential",

"iam:UpdateServiceSpecificCredential"

],

"Resource": "arn:aws:iam::\*:user/${aws:username}"

},

{

"Sid": "AllowManageOwnVirtualMFADevice",

"Effect": "Allow",

"Action": [

"iam:CreateVirtualMFADevice"

],

"Resource": "arn:aws:iam::\*:mfa/\*"

},

{

"Sid": "AllowManageOwnUserMFA",

"Effect": "Allow",

"Action": [

"iam:DeactivateMFADevice",

"iam:EnableMFADevice",

"iam:ListMFADevices",

"iam:ResyncMFADevice"

],

"Resource": "arn:aws:iam::\*:user/${aws:username}"

},

{

"Sid": "DenyAllExceptListedIfNoMFA",

"Effect": "Deny",

"NotAction": [

"iam:CreateVirtualMFADevice",

"iam:EnableMFADevice",

"iam:GetUser",

"iam:ListMFADevices",

"iam:ListVirtualMFADevices",

"iam:ResyncMFADevice",

"sts:GetSessionToken"

],

"Resource": "\*",

"Condition": {

"BoolIfExists": {

"aws:MultiFactorAuthPresent": "false"

}

}

}

]

}