**SCP applied at OU Level**

{

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

"Statement": [

{

"Sid": "DenyEC2NetworkingActions",

"Effect": "Deny",

"Action": [

"ec2:ReplaceRouteTableAssociation",

"ec2:DeleteClientVpnEndpoint",

"ec2:CreateTransitGatewayConnect",

"ec2:CreateTransitGatewayRouteTable",

"ec2:ModifyTransitGateway",

"ec2:ModifyClientVpnEndpoint",

"ec2:RejectTransitGatewayMulticastDomainAssociations",

"ec2:CreateTransitGatewayConnectPeer",

"ec2:AttachInternetGateway",

"ec2:AcceptTransitGatewayVpcAttachment",

"ec2:DisableVgwRoutePropagation",

"ec2:CreateTransitGateway",

"ec2:ReplaceRoute",

"ec2:UnassignPrivateNatGatewayAddress",

"ec2:DeleteRouteTable",

"ec2:CreateTransitGatewayPrefixListReference",

"ec2:ModifyVpnConnectionOptions",

"ec2:CreateTransitGatewayPeeringAttachment",

"ec2:DeleteTransitGatewayVpcAttachment",

"ec2:DeleteVpnGateway",

"ec2:ModifyTransitGatewayPrefixListReference",

"ec2:CreateRoute",

"ec2:CreateInternetGateway",

"ec2:CreateTransitGatewayMulticastDomain",

"ec2:CreateVpnGateway",

"ec2:AssociateTransitGatewayRouteTable",

"ec2:DeleteInternetGateway",

"ec2:RejectTransitGatewayVpcAttachment",

"ec2:DeleteVpnConnection",

"ec2:CreateVpcPeeringConnection",

"ec2:DeleteTransitGatewayRouteTableAnnouncement",

"ec2:DisassociateTransitGatewayRouteTable",

"ec2:DisassociateTransitGatewayPolicyTable",

"ec2:DisableTransitGatewayRouteTablePropagation",

"ec2:DeleteTransitGatewayPeeringAttachment",

"ec2:DeregisterTransitGatewayMulticastGroupMembers",

"ec2:CreateRouteTable",

"ec2:CreateTransitGatewayRouteTableAnnouncement",

"ec2:DetachInternetGateway",

"ec2:AssociateClientVpnTargetNetwork",

"ec2:DisassociateRouteTable",

"ec2:CreateTransitGatewayPolicyTable",

"ec2:DeleteTransitGatewayRouteTable",

"ec2:DetachVpnGateway",

"ec2:CreateTransitGatewayRoute",

"ec2:DeleteTransitGatewayRoute",

"ec2:CreateTransitGatewayVpcAttachment",

"ec2:DeleteNatGateway",

"ec2:AssignPrivateNatGatewayAddress",

"ec2:DeleteVpc",

"ec2:CreateEgressOnlyInternetGateway",

"ec2:EnableTransitGatewayRouteTablePropagation",

"ec2:DeleteTransitGateway",

"ec2:CreateVpnConnection",

"ec2:DeleteTransitGatewayPrefixListReference",

"ec2:ModifyLocalGatewayRoute",

"ec2:ExportTransitGatewayRoutes",

"ec2:CreateNatGateway",

"ec2:DeleteTransitGatewayPolicyTable",

"ec2:AcceptTransitGatewayPeeringAttachment",

"ec2:CreateVpc",

"ec2:ModifyVpnConnection",

"ec2:ReplaceTransitGatewayRoute",

"ec2:DeleteTransitGatewayMulticastDomain",

"ec2:RejectTransitGatewayPeeringAttachment",

"ec2:RegisterTransitGatewayMulticastGroupSources",

"ec2:TerminateClientVpnConnections",

"ec2:DeregisterTransitGatewayMulticastGroupSources",

"ec2:ModifyVpnTunnelCertificate",

"ec2:ReplaceVpnTunnel",

"ec2:DeleteTransitGatewayConnectPeer",

"ec2:AssociateNatGatewayAddress",

"ec2:ModifyTransitGatewayVpcAttachment",

"ec2:DeleteEgressOnlyInternetGateway",

"ec2:DisassociateTransitGatewayMulticastDomain",

"ec2:DisassociateClientVpnTargetNetwork",

"ec2:CreateClientVpnRoute",

"ec2:AttachVpnGateway",

"ec2:DeleteRoute",

"ec2:AssociateTransitGatewayMulticastDomain",

"ec2:CreateVpnConnectionRoute",

"ec2:RevokeClientVpnIngress",

"ec2:RegisterTransitGatewayMulticastGroupMembers",

"ec2:CreateClientVpnEndpoint",

"ec2:DeleteVpnConnectionRoute",

"ec2:AuthorizeClientVpnIngress",

"ec2:DisassociateNatGatewayAddress",

"ec2:ModifyVpnTunnelOptions",

"ec2:ImportClientVpnClientCertificateRevocationList",

"ec2:AssociateTransitGatewayPolicyTable",

"ec2:DeleteClientVpnRoute",

"ec2:EnableVgwRoutePropagation",

"ec2:DeleteTransitGatewayConnect",

"ec2:AcceptTransitGatewayMulticastDomainAssociations"

],

"Resource": "\*"

}

]

}

**IAM Policy (added a few EC2 related permissions at the end w.r.t. roles)**

{

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

"Statement": [

{

"Effect": "Allow",

"NotAction": [

"iam:\*",

"organizations:\*",

"account:\*"

],

"Resource": "\*"

},

{

"Effect": "Allow",

"Action": [

"iam:PassRole"

],

"Resource": "arn:aws:iam::(AccountID):role/\*"

},

{

"Effect": "Allow",

"Action": [

"organizations:DescribeOrganization",

"account:ListRegions",

"account:GetAccountInformation",

"iam:List\*",

"iam:Get\*",

"iam:CreateRole",

"iam:UpdateRole",

"iam:DeleteRole",

"iam:Attach\*",

"iam:CreatePolicy",

"iam:CreatePolicyVersion",

"iam:DeletePolicy",

"iam:DeletePolicyVersion",

"iam:CreateInstanceProfile",

"iam:DeleteInstanceProfile",

"iam:AddRoleToInstanceProfile",

"iam:RemoveRoleFromInstanceProfile",

"iam:Tag\*",

"iam:Untag\*",

"ec2:AssociateIamInstanceProfile",

"ec2:DisassociateIamInstanceProfile",

"ec2:ReplaceIamInstanceProfileAssociation"

],

"NotResource": [

"arn:aws:iam::\*:role/sse-aws-role-bu-terraformcloud-admin",

"arn:aws:iam::\*:role/aws-reserved/\*"

]

}

]

}

**Permission Boundary to Attach (once it is attached, the role cannot remove or alter it. Also it cannot create more users or roles without attaching this boundary so a permission ceiling will always be present)**

{

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

"Statement": [

{

"Effect": "Allow",

"NotAction": [

"iam:\*",

"organizations:\*",

"account:\*"

],

"Resource": "\*"

},

{

"Effect": "Allow",

"Action": [

"iam:PassRole"

],

"Resource": "arn:aws:iam::(AccountID):role/\*"

},

{

"Effect": "Allow",

"Action": [

"organizations:DescribeOrganization",

"account:ListRegions",

"account:GetAccountInformation",

"iam:List\*",

"iam:Get\*",

"iam:CreateRole",

"iam:UpdateRole",

"iam:DeleteRole",

"iam:Attach\*",

"iam:CreatePolicy",

"iam:CreatePolicyVersion",

"iam:DeletePolicy",

"iam:DeletePolicyVersion",

"iam:CreateInstanceProfile",

"iam:DeleteInstanceProfile",

"iam:AddRoleToInstanceProfile",

"iam:RemoveRoleFromInstanceProfile",

"iam:Tag\*",

"iam:Untag\*",

"ec2:AssociateIamInstanceProfile",

"ec2:DisassociateIamInstanceProfile",

"ec2:ReplaceIamInstanceProfileAssociation"

],

"NotResource": [

"arn:aws:iam::\*:role/sse-aws-role-bu-terraformcloud-admin",

"arn:aws:iam::\*:role/aws-reserved/\*"

]

},

{

"Sid": "DenyPermissionBoundaryAlteration",

"Effect": "Deny",

"Action": [

"iam:DeletePolicy",

"iam:DeletePolicyVersion",

"iam:CreatePolicyVersion",

"iam:SetDefaultPolicyVersion"

],

"Resource": [

"arn:aws:iam::(AccountID):policy/SSE-permissionBoundary"

]

},

{

"Sid": "DenyRemovalOfBoundary",

"Effect": "Deny",

"Action": [

"iam:DeleteRolePermissionsBoundary",

"iam:DeleteUserPermissionsBoundary"

],

"Resource": [

"arn:aws:iam::(AccountID):user/\*",

"arn:aws:iam::(AccountID):role/\*"

],

"Condition": {

"StringEquals": {

"iam:PermissionsBoundary": "arn:aws:iam::(AccountID):policy/SSE-permissionBoundary"

}

}

},

{

"Sid": "DenyIfBoundaryNotApplied",

"Effect": "Deny",

"Action": [

"iam:PutUserPermissionsBoundary",

"iam:PutRolePermissionsBoundary"

],

"Resource": [

"arn:aws:iam::(AccountID):user/\*",

"arn:aws:iam::(AccountID):role/\*"

],

"Condition": {

"StringNotEquals": {

"iam:PermissionsBoundary": "arn:aws:iam::(AccountID):policy/SSE-permissionBoundary"

}

}

},

{

"Sid": "DenyUserandRoleCreationWithoutBoundary",

"Effect": "Deny",

"Action": [

"iam:CreateRole",

"iam:CreateUser"

],

"Resource": [

"arn:aws:iam::(AccountID):user/\*",

"arn:aws:iam::(AccountID):role/\*"

],

"Condition": {

"StringNotEquals": {

"iam:PermissionsBoundary": "arn:aws:iam::(AccountID):policy/SSE-permissionBoundary"

}

}

}

]

}