**SOP for Security Groups to Restrict Traffic between Internet and Amazon VPC:**

**Objective:** This SOP provides guidelines and procedures to ensure the security of the Virtual Private Cloud (Amazon VPC) and secure traffic within the VPC by implementing security groups. This also includes samples for private & public servers along with the DB servers

**Scope:** This SOP applies to all AWS accounts and personnel responsible for managing and securing Amazon VPCs.

| **Roles** | **Responsibilities** |
| --- | --- |
| AWS Account Owner | Responsible for managing the overall security of Amazon VPCs. |
| AWS VPC Administrator | Responsible for implementing and maintaining security groups and network ACLs within Amazon VPCs. |
| Network Security Team | Responsible for reviewing and approving security configurations and conducting periodic audits. |

**Security Groups to Restrict Traffic between Internet and Amazon VPC:**

Create security groups to control inbound and outbound traffic between the internet and Amazon VPC.

Configure security group rules to allow necessary inbound traffic while blocking unauthorized access.

Deny all inbound traffic by default and only allow explicitly permitted traffic.

Regularly review and update security group rules based on changing security requirements.

Document the security group configurations, including rules, allowed ports, and traffic sources.

**Procedure:**

**Define Security Best Practices for Amazon VPC:**

Amazon VPC provides a secure and isolated virtual network environment. The following security best practices should be followed:

| Best Practices | Links |
| --- | --- |
| Enable Multi-Factor Authentication (MFA) for AWS accounts with administrative privileges: | <https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable_virtual.html> |
| Implement strong password policies and enforce password rotation for IAM users: | <https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html> |
| Use AWS Identity and Access Management (IAM) roles to assign appropriate permissions to resources: | <https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user.html> |
| Enable AWS CloudTrail to log and monitor API activity within the VPC: | <https://docs.aws.amazon.com/AWSEC2/latest/APIReference/using-cloudtrail.html> |
| Enable VPC Flow Logs to capture information about IP traffic for auditing and troubleshooting purposes: | <https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html> |
| Encrypt sensitive data in transit using SSL/TLS protocols: | <https://cloud.google.com/docs/security/encryption-in-transit> |
| Regularly review security group and network ACL configurations to ensure they align with security requirements: | <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-security-groups.html>  <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html> |

**Sample Examples are as below:**

When you create a security group, you must provide it with a name and a description. The following rules apply:

* A security group name must be unique within the VPC.
* Names and descriptions can be up to 255 characters in length.
* Names and descriptions are limited to the following characters: a-z, A-Z, 0-9, spaces, and .\_-:/()#,@[]+=&;{}!$\*.
* When the name contains trailing spaces, we trim the space at the end of the name. For example, if you enter "Test Security Group " for the name, we store it as "Test Security Group".
* A security group name cannot start with SG

**Common Security Group Rules**

| **Rule** | **Description** |
| --- | --- |
| Default Inbound | By default, all inbound traffic is denied. |
| SSH (TCP 22) | Allow SSH access for remote administration. |
| HTTP (TCP 80) | Allow inbound HTTP traffic for web servers. |
| HTTPS (TCP 443) | Allow inbound HTTPS traffic for secure web servers. |
| RDP (TCP 3389) | Allow RDP access for Windows instances. |
| **Custom Ports** | **Allow specific ports required by applications or services.**  **Any custom ports addition apart from above would need explicit email approval from the customer for the same with source iP restriction.** |

**Common Security Group Best Practices:**

* Allow only necessary inbound ports based on the services offered.
* Limit access to SSH and RDP ports to trusted IP addresses or administrative networks.
* Use Security Groups to restrict communication between different tiers of multi-tier applications.
* Restrict outbound traffic to necessary destinations only.

**Common Network ACL Rules**

| **Rule** | **Description** |
| --- | --- |
| Default Inbound | By default, all inbound traffic is denied. |
| Default Outbound | By default, all outbound traffic is allowed. |
| Custom Rules | Custom rules to allow or deny specific traffic patterns.  Customers may request their office location to be connected Ideally this should be routed via Site to Site VPN (if implemented), if not then be specific about the IP Block/ range with appropriate Subnet Mask as explicitly signed-off with the client on email and add accordingly in the allowed IP range. |
| Logging | Enable logging of denied traffic for analysis. |
| Rule Order | Rules are evaluated based on their rule number (priority). |

**Common Network ACL Best Practices:**

* Use Network ACLs to add an extra layer of security at the subnet level.
* Consider logging denied traffic for analysis and monitoring purposes.
* Regularly review and audit Network ACL configurations for accuracy and compliance.
* Be cautious when modifying Network ACLs, as they can impact all resources within the subnet.

**Sample Example of the Security Group for Public/Web servers**

The following security group rules allow the web servers to receive HTTP and HTTPS traffic from clients, from all IPv4 and IPv6 addresses. You can optionally allow the web servers to receive SSH or RDP traffic from your network. The web servers can also send SQL or MySQL traffic to your database servers.

| **Inbound** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Source** | **Protocol** | **Port range** | **Description** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 0.0.0.0/0 | TCP | 80 | Allows inbound HTTP access from all IPv4 addresses |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| ::/0 | TCP | 80 | Allows inbound HTTP access from all IPv6 addresses |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 0.0.0.0/0 | TCP | 443 | Allows inbound HTTPS access from all IPv4 addresses |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| ::/0 | TCP | 443 | Allows inbound HTTPS access from all IPv6 addresses |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| *Public IPv4 address range of your network* | TCP | 22 | (Optional) Allows inbound SSH access from IPv4 IP addresses in your network |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| *IPv6 address range of your network* | TCP | 22 | (Optional) Allows inbound SSH access from IPv6 IP addresses in your network |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| *Public IPv4 address range of your network* | TCP | 3389 | (Optional) Allows inbound RDP access from IPv4 IP addresses in your network |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| *IPv6 address range of your network* | TCP | 3389 | (Optional) Allows inbound RDP access from IPv6 IP addresses in your network |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

| **Outbound** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Destination** | **Protocol** | **Port range** | **Description** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| *ID of the security group for instances running Microsoft SQL Server* | TCP | 1433 | Allows outbound Microsoft SQL Server access |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| *ID of the security group for instances running MySQL* | TCP | 3306 | Allows outbound MySQL access |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

**Sample Example of the Security Group for Database servers**

The following security group rules allow the database servers to receive read and write requests from the web servers.

| **Inbound** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Source** | **Protocol** | **Port range** | **Comments** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| *ID of the web server security group* | TCP | 1433 | Allows inbound Microsoft SQL Server access from the web servers |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| *ID of the web server security group* | TCP | 3306 | Allows inbound MySQL Server access from the web servers |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

| **Outbound** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Destination** | **Protocol** | **Port range** | **Comments** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 0.0.0.0/0 | TCP | 80 | Allows outbound HTTP access to the internet over IPv4 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 0.0.0.0/0 | TCP | 443 | Allows outbound HTTPS access to the internet over IPv4 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

**Sample Example of the Security Group for Private servers**

The following is an example of the rules that you might create for the security group that you associate with your servers. The security group must allow traffic from the load balancer over the listener port and protocol. It must also allow health check traffic.

| **Inbound** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Source** | **Protocol** | **Port range** | **Comments** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| *ID of the load balancer security group* | *listener protocol* | *listener port* | Allows inbound traffic from the load balancer on the listener port |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| *ID of the load balancer security group* | *health check protocol* | *health check port* | Allows inbound health check traffic from the load balancer |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

**Sample Example of the NACL for VPC**

The following example shows a custom network ACL for a **VPC that supports IPv4 only**. It includes inbound rules that allow HTTP and HTTPS traffic (100 and 110). There's a corresponding outbound rule that enables responses to that inbound traffic (140), which covers ephemeral ports 32768-65535. For more information about how to select the appropriate ephemeral port range.

The network ACL also includes inbound rules that allow SSH and RDP traffic into the subnet. Outbound rule 120 enables responses to leave the subnet.

The network ACL has outbound rules (100 and 110) that allow outbound HTTP and HTTPS traffic out of the subnet. There's a corresponding inbound rule that enables responses to that outbound traffic (140), which covers ephemeral ports 32768-65535.

Each network ACL includes a default rule whose rule number is an asterisk. This rule ensures that if a packet doesn't match any of the other rules, it's denied. You can't modify or remove this rule.

| **Inbound** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Rule #** | **Type** | **Protocol** | **Port range** | **Source** | **Allow/Deny** | **Comments** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 100 | HTTP | TCP | 80 | 0.0.0.0/0 | ALLOW | Allows inbound HTTP traffic from any IPv4 address. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 110 | HTTPS | TCP | 443 | 0.0.0.0/0 | ALLOW | Allows inbound HTTPS traffic from any IPv4 address. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 120 | SSH | TCP | 22 | 192.0.2.0/24 | ALLOW | Allows inbound SSH traffic from your home network's public IPv4 address range (over the internet gateway). |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 130 | RDP | TCP | 3389 | 192.0.2.0/24 | ALLOW | Allows inbound RDP traffic to the web servers from your home network's public IPv4 address range (over the internet gateway). |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 140 | Custom TCP | TCP | 32768-65535 | 0.0.0.0/0 | ALLOW | Allows inbound return IPv4 traffic from the internet (that is, for requests that originate in the subnet).  This range is an example only. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| \* | All traffic | All | All | 0.0.0.0/0 | DENY | Denies all inbound IPv4 traffic not already handled by a preceding rule (not modifiable). |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

| **Outbound** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Rule #** | **Type** | **Protocol** | **Port range** | **Destination** | **Allow/Deny** | **Comments** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 100 | HTTP | TCP | 80 | 0.0.0.0/0 | ALLOW | Allows outbound IPv4 HTTP traffic from the subnet to the internet. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 110 | HTTPS | TCP | 443 | 0.0.0.0/0 | ALLOW | Allows outbound IPv4 HTTPS traffic from the subnet to the internet. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 120 | SSH | TCP | 1024-65535 | 192.0.2.0/24 | ALLOW | Allows outbound SSH traffic from your home network's public IPv4 address range (over the internet gateway). |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 140 | Custom TCP | TCP | 32768-65535 | 0.0.0.0/0 | ALLOW | Allows outbound IPv4 responses to clients on the internet (for example, serving webpages to people visiting the web servers in the subnet).  This range is an example only. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| \* | All traffic | All | All | 0.0.0.0/0 | DENY | Denies all outbound IPv4 traffic not already handled by a preceding rule (not modifiable). |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

As a packet comes to the subnet, we evaluate it against the inbound rules of the ACL that the subnet is associated with (starting at the top of the list of rules, and moving to the bottom). Here's how the evaluation goes if the packet is destined for the HTTPS port (443). The packet doesn't match the first rule evaluated (rule 100). It does match the second rule (110), which allows the packet into the subnet. If the packet had been destined for port 139 (NetBIOS), it doesn't match any of the rules, and the \* rule ultimately denies the packet.

You might want to add a deny rule in a situation where you legitimately need to open a wide range of ports, but there are certain ports within the range that you want to deny. Just make sure to place the deny rule earlier in the table than the rule that allows the wide range of port traffic.

You add allow rules depending on your use case. For example, you can add a rule that allows outbound TCP and UDP access on port 53 for DNS resolution. For every rule that you add, ensure that there is a corresponding inbound or outbound rule that allows response traffic.