保护 AWS 云中您的 VPC 的出站网络流量

AWS 规范性指导

AWS 规范性指导: 保护 AWS 云中您的 VPC 的出站网络流量

Table of Contents

保护 AWS 云中您的 VPC 的出站网络流量

Kirankumar Chandrashekar and Abdal Garuba, Amazon Web Services（AWS）

2022 年 11 月（文档历史记录）

本指南介绍使用 Amazon Virtual Private Cloud（Amazon VPC）保护和监控出站网络流量的最佳实践。它还介绍了可帮助您监控来自弹性网络接口和云中虚拟私有云 (VPCs) 的出站网络流量的 AWS 工具。 AWS

> **注意**
>
> 本指南不涵盖可以与之集成 AWS 以提供更多安全层的第三方工具。本指南假设您采用的是仅使用云的架构。本指南不适用于混合架构。

本指南概述了以下最佳实践：

- 通过分析现有流量模式确定您 VPC 的安全要求
- 使用安全组限制 VPC 的出站流量
- 使用 AWS Network Firewall 和 DNS 主机名限制 VPC 的出站流量
- 使用 VPC 终端节点访问 AWS 资源
- 使用在内部应用程序之间建立私有连接 AWS PrivateLink
- 使用 VPC 对 VPCs 等 AWS 区域 互连或使用 VPC 对等互连进行通信或 AWS Transit Gateway

> **注意**
>
> 为了获得最佳的安全状态，您还可以通过专用路径将出站流量传递到筛选工具，例如防火墙设备。

目标业务成果

本指南可以帮助您执行以下操作：

1. 控制和监控您的 VPC 的出站网络流量。

2. 确保 AWS 资源之间的流量通过由 AWS 主干网络控制的安全、私有路由。
3. 实施 AWS 工具来持续监控出站网络流量，并阻止向未经批准的终端节点发出的请求。

确定您 VPC 的安全要求

> **重要提示**
>
> 在测试环境中设计和测试 VPC 的出站流量安全架构是一种最佳实践。在开发环境中测试架构变更可以减轻推送意外系统行为的实时风险。

在更改网络的出站流量模式之前，请务必了解应用程序按预期运行所需的流量模式。这些信息可以帮助您确定在重新架构网络时允许哪些流量模式和拒绝哪些流量模式。

要分析您的 VPC 现有的出站流量模式，请先打开 VPC 流日志。然后，使用测试环境在各种使用场景中运行您的应用程序，并分析流日志中的模拟流量。

VPC 流日志会记录您的 VPC 的入站和出站 IP 流量。然后，亚马逊 VPC 将日志发送到亚马逊简单存储服务 (Amazon S3) 或亚马逊。 CloudWatch您可以使用以下任一工具查看和分析日志：

- （适用于 Amazon S3）Amazon Athena
- （适用于 CloudWatch）CloudWatch 日志见解

有关更多信息和查询示例，请参阅以下内容：

- 查询 Amazon VPC 流日志（Amazon Athena 用户指南）
- 如何在我的 VPC 流 CloudWatch 日志中使用日志见解查询？（AWS 知识中心）
- CloudWatch 日志见解查询语法（Amazon CloudWatch 日志用户指南）

有关 VPC 流日志捕获的信息类型的详细信息，请参阅 Amazon VPC 用户指南中的流日志记录示例。

> **注意**
>
> VPC 流日志不会捕获应用程序层（第 7 层）信息，例如 DNS 主机名。如果您的安全要求需要分析应用程序层数据，则可以部署 AWS Network Firewall 以捕获所需的详细信息。有关更多信息，请参阅本指南的使用 AWS Network Firewall 和 DNS 主机名限制 VPC 的出站流量部分。

使用 VPC 流日志分析您的 VPC 的出站流量的最佳实践

使用 Amazon Athena CloudWatch 或 Logs Insights 查询分析您的 VPC 流日志时，请务必执行以下操作：

- 确定和分析流经连接到您的应用程序使用的资源的弹性网络接口的入站和出站流量。
- 确定和分析流经连接到 NAT 网关的网络接口的应用程序流量。
- 通过将查询中的源地址设为网络接口的私有 IP 地址，确保捕获到网络接口的所有出站流量。
- 写入您的查询，仅关注意外流量模式。（例如，如果您的应用程序与第三方实体（例如 HTTPS API 端点）进行通信，则您可以在构造查询时不包含这些实体。）
- 调查每个端口和目标 IP 地址的有效性。（例如，对于堡垒主机或者使用 SSH 从 Git 克隆存储库的主机而言，出站目标端口 22 可能是正常的。）

> **注意**
>
> 如果您是首次使用 Amazon Athena，请务必配置查询结果位置。有关其说明，请参阅 Amazon Athena 用户指南中的使用 Athena 控制台指定查询结果位置。

Amazon Athena 查询示例

返回来自特定网络接口的出站管理员流量的 Athena 查询示例

以下 Athena 查询返回来自网络接口的前 200 条出站管理员流量的结果，该网络接口的 IP 地址为 10.100.0.10：

```
SELECT * FROM "<vpc_flow_logs_table_name>"

WHERE interface_id = 'eni-1234567890000000' AND srcaddr LIKE '10.100.0.10' AND dstport
 < 1024

LIMIT 200;
```

输出示例

#	1

version	2
account_id	<account-id>
interface_id	eni-123456789000000
srcaddr	10.32.0.10
dstaddr	11.22.33.44
srcport	36952
dstport	443
protocol	6
packets	25
bytes	5445
start	1659310200
end	1659310225
action	ACCEPT
log_status	OK
date	2022-07-16

> **注意**
>
> 此模式中的输出格式仅用于演示目的，在您的系统上可能会有所不同。

返回从特定 VPC 接收最多流量的外部 IP 地址的 Athena 查询示例

以下 Athena 查询可以返回从 VPC 接收最多出站流量的外部 IP 地址和端口，CIDR 块以“10.32”开头：

```
SELECT dstport, dstaddr,
```

```
count(*) AS count

FROM "<vpc_flow_logs_table_name>"

WHERE dstaddr not like '10.32%' AND interface_id = 'eni-1234567890000000'

GROUP BY dstport, dstaddr

ORDER BY count desc

LIMIT 200;
```

输出示例

#	Dstport	Dstaddr	count
1	443	52.x.x.x	1442
2	443	63.x.x.x	1201
3	443	102.x.x.x	887

返回来自特定 VPC 的被拒绝的出站流量的 Athena 查询示例

以下 Athena 查询可以返回来自 VPC 的被拒绝的出站流量，CIDR 块以“10.32”开头：

```
SELECT *

FROM "<vpc_flow_logs_table_name>"

WHERE srcaddr like '10.32%' AND action LIKE 'REJECT'
```

输出示例

#	1
version	2
account_id	<account-id>

interface_id	eni-123456789000000
srcaddr	10.32.0.10
dstaddr	11.22.33.44
srcport	36952
dstport	443
protocol	6
packets	25
bytes	5445
start	1659310200
end	1659310225
action	REJECT
log_status	OK
date	2022-07-16

> **注意**
>
> 此模式中的输出格式仅用于演示目的，在您的系统上可能会有所不同。

有关如何解读 Athena 查询结果的更多信息，请参阅 Amazon VPC 用户指南中的流日志记录。

CloudWatch 日志见解查询示例

CloudWatch Logs Insights 查询示例，该示例返回来自特定网络接口的出站管理员流量

以下 CloudWatch Logs Insights 查询返回来自 IP 地址为 10.100. 0.10 的网络接口的出站管理员流量的前 200 个结果：

```
fields @timestamp, @message
```

```
| filter interfaceId = 'eni-1234567890000000'

| filter srcAddr = '10.100.0.10'

| filter dstPort < 1024

| limit 200
```

输出示例

Field	Value
@ingestionTime	1659310250813
@log	<account-id>:/aws/vpc/flowlogs
@logStream	eni-123456789000000-all
@message	2 <account-id> eni-123456789000000 10.100.0.10 11.22.33.44 36952 443 6 25 5445 1659310200 1659310225 ACCEPT OK
@timestamp	1659310200000
accountId	<account-id>
action	ACCEPT
bytes	5445
dstAddr	11.22.33.44
dstPort	443
end	1659310225
interfaceId	eni-123456789000000
logStatus	OK
packets	25

protocol	6
srcAddr	10.100.0.10
srcPort	36952
start	1659310200
version	2

示例 CloudWatch Logs Insights 查询，该查询返回来自特定 VPC 的流量最多的外部 IP 地址

以下 CloudWatch Logs Insights 查询返回从 CIDR 块以 '10.32' 开头的 VPC 接收最多出站流量的外部 IP 地址和端口：

```
filter @logstream = 'eni-1234567890000000'

| stats count(*) as count by dstAddr, dstPort

| filter dstAddr not like '10.32'

| order by count desc

| limit 200
```

输出示例

#	dstAddr	dstPort	count
1	52.x.x.x	443	439
2	51.79.x.x	63.x.x.x	25

返回来自特定 VPC 的被拒绝出站流量的 CloudWatch 日志洞察查询示例

以下 CloudWatch Logs Insights 查询返回来自 CIDR 块以 '10.32' 开头的 VPC 的被拒绝的出站流量：

```
filter @logstream = 'eni-0123456789000000'

| fields @timestamp, @message
```

```
| filter action='REJECT'
```

输出示例

Field	Value
@ingestionTime	1666991000899
@log	<account-id>:/aws/vpc/flowlogs
@logStream	eni-0123456789000000-all
@message	2 <account-id> 'eni-0123456789000000' 185.x.x.x 10.10.2.222 55116 11211 17 1 43 1666990939 1666990966 REJECT OK
@timestamp	1666990939000
accountId	<account-id>
action	REJECT
bytes	43
dstAddr	10.10.2.222
dstPort	11211
end	1666990966
interfaceId	'eni-0123456789000000'
logStatus	OK
数据包	1
protocol	17
srcAddr	185.x.x.x
srcPort	55116

start	1666990939
version	2

限制 VPC 的出站流量

使用安全组限制 VPC 的出站流量

评估架构的出站流量要求后，开始修改 VPC 的安全组规则以满足组织的安全需求。确保将所有必要的端口、协议和目标 IP 地址添加到安全组的允许列表中。

有关其说明，请参阅 Amazon VPC 用户指南中的使用安全组控制到资源的流量。

> **重要提示**
>
> 在测试环境中更新 VPC 的安全组规则后，请务必确认您的应用程序仍按预期运行。有关更多信息，请参阅本指南的使用 VPC 流日志分析您的 VPC 出站流量的最佳实践部分。

特定 AWS 服务的关键安全组注意事项

Amazon Elastic Compute Cloud（Amazon EC2）

创建 VPC 时，它带有一个允许所有出站流量的默认安全组。Amazon Elastic Compute Cloud（Amazon EC2）实例默认使用此安全组，除非您创建自己的自定义安全组。

> **重要提示**
>
> 要减轻您的 Amazon EC2 实例无意中使用默认安全组的风险，请移除该组的所有出站规则。有关更多信息，请参阅 Amazon VPC 用户指南中使用安全组规则部分中的删除安全组规则。

Amazon Relational Database Service（Amazon RDS）

除非数据库充当客户端，否则所有 Amazon RDS DB 实例的出站安全组规则都可以删除。有关更多信息，请参阅 Amazon RDS 用户指南中的 VPC 安全组概述。

Amazon ElastiCache

亚马逊 ElastiCache (Redis OSS) 和亚马逊 ElastiCache (Memcached) 实例的所有出站安全组规则都可以删除，除非该实例充当客户端。有关更多信息，请参阅下列内容：

- 安全组： EC2-Classic（亚马逊 ElastiCache （Redis OSS）用户指南）
- 了解 ElastiCache 和亚马逊 VPC（亚马逊 ElastiCache (Memcached) 用户指南）

使用限制 VPC 的出站流量 AWS Network Firewall 和 DNS 主机名

当应用程序使用动态 IP 地址时，最佳实践是使用 DNS 主机名来筛选其 VPC 的出站流量，而不是使用 IP 地址。例如，如果应用程序正在使用应用程序负载均衡器，则该应用程序的关联 IP 地址将发生变化，因为节点会不断扩展。在这种情况下，使用 DNS 主机名筛选出站网络流量比使用静态 IP 地址更安全。

您可以使用 AWS Network Firewall 将您的 VPC 的出站互联网访问限制为一组主机名，由 HTTPS 流量中的服务器名称指示（SNI）提供。

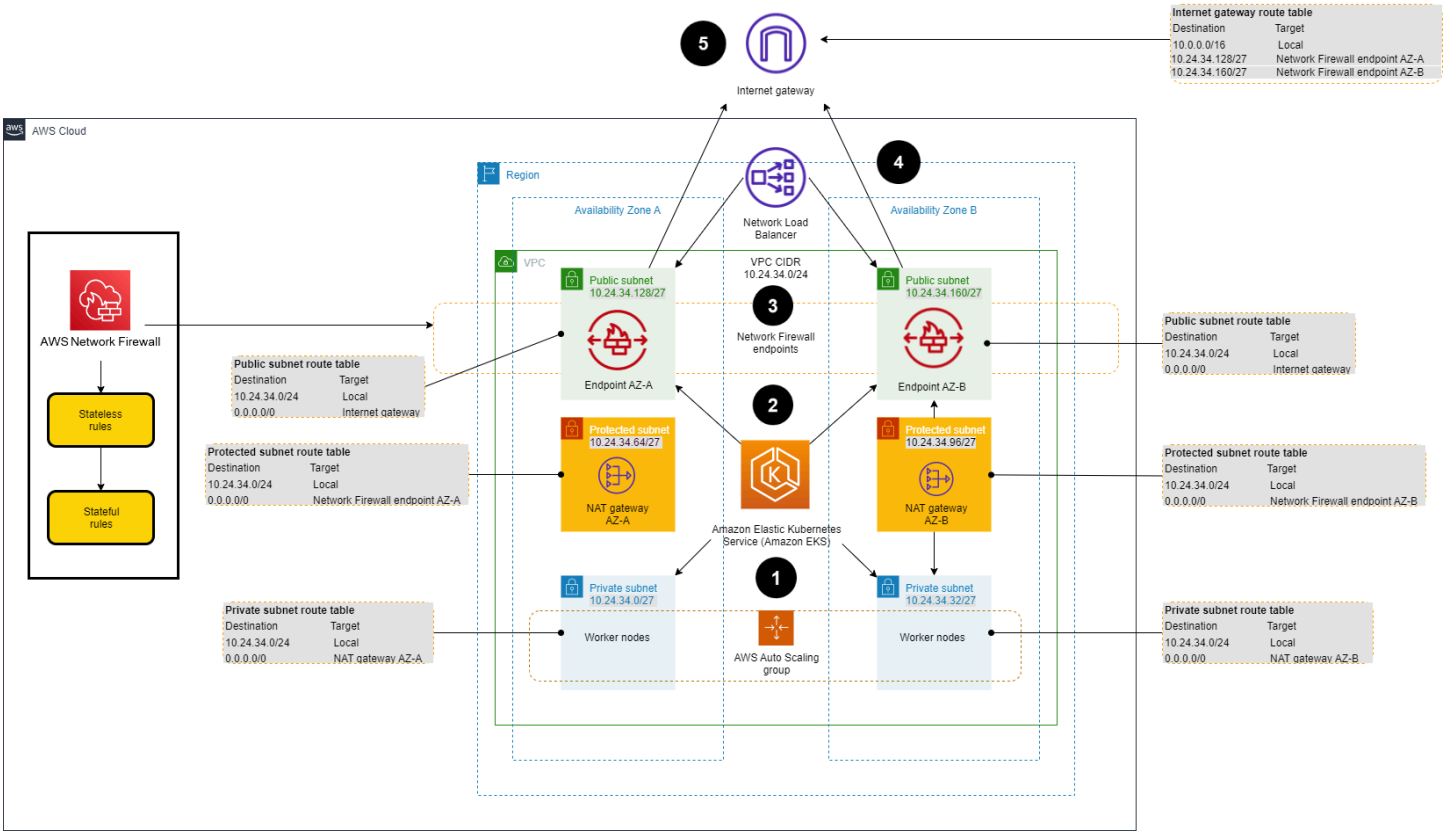
有关更多信息和 Network Firewall 策略规则示例，请参阅 AWS Network Firewall 开发者指南中的域筛选。有关详细说明，请参阅以下 AWS Prescriptive Guidance（APG）模式：使用 Network Firewall 从出站流量的服务器名称指示（SNI）捕获 DNS 域名。

> **备注**
>
> SNI 是 TLS 的扩展，在流量中保持未加密状态。它表示客户端试图通过 HTTPS 访问的目标主机名。

> **重要提示**
>
> 在测试环境中更新 Network Firewall 状态规则后，请确保您的应用程序仍按预期运行。确保 SNI 提供的必需的 DNS 域名均未被阻止。

架构示例

下图显示了使用 AWS Network Firewall DNS 主机名过滤 VPC 出站流量的示例架构：



下图显示了如下工作流：

1. 出站请求从私有子网内发出，然后发送到受保护子网中的 NAT 网关。
2. NAT 网关收到的 HTTPS 流量将路由到公有子网中的 AWS Network Firewall 终端节点。
3. AWS Network Firewall 检查请求并应用配置的防火墙策略规则来接受或拒绝传递到 Internet 网关的请求。
4. 经批准的出站请求将发送到互联网网关。
5. 来自互联网网关的经批准的流量将被发送到互联网以访问预期的 URL（由 SNI 在非加密的 HTTPS 标头中提供）。

访问 AWS 资源

VPC 终端节点在 VPC 和支持的 AWS 服务之间提供私有连接，无需互联网网关或 NAT 网关。例如，您可以使用 VPC 端点将 VPC 连接到 Amazon Simple Storage Service（Amazon S3）或 Amazon Elastic Container Registry（Amazon ECR）。

Amazon VPC 提供三种类型的 VPC 端点：

- 接口终端节点 VPCs 连接到支持的 Amazon VPC 服务 AWS PrivateLink。
- 网关端点，其专门提供与 Amazon S3 和 Amazon DynamoDB 之间的可靠连接。
- Gateway Load Balancer 端点 VPCs 连接到托管在 Gateway Load Balancer 后面的自定义应用程序。

有关支持的服务列表，请参阅 Amazon VPC 文档中的与 AWS PrivateLink集成的AWS 服务。

> **注意**
>
> Gateway Load Balancer 终端节点在私下与应用程序 VPC 或 AWS 账户之外的用户共享应用程序时非常有用。有关更多信息，请参阅本指南的在内部应用程序之间建立私有连接部分。

在内部应用程序之间建立私有连接

通过使用 AWS PrivateLink，可以在云端私下共享基于 AWS 云的应用程序的端点。有关更多信息以及示例架构，请参阅 AWS PrivateLink 文档。

有关架构的更多示例，请参阅以下 AWS 规范性指导模式：

- 使用 AWS PrivateLink 和 Network Load Balancer 在 Amazon ECS 上私密访问容器应用程序
- 使用 AWS Fargate、 AWS PrivateLink和 Network Load Balancer 在 Amazon ECS 上私密访问容器应用程序
- 使用 AWS PrivateLink 和 Network Load Balancer 在 Amazon EKS 上私密访问容器应用程序

跨界 VPCs 沟通 AWS 区域

多 VPC 基础设施可以帮助组织划分工作负载并扩大其覆盖范围。当资源需要与不同的、和 AWS 账户中的 AWS 服务通信时 VPCs AWS 区域，这种架构也可能带来挑战。

要在两者之间建立连接 VPCs，可以使用 VPC 对等或AWS Transit Gateway。VPC 对等连接是两者之间的网络连接，它使用私 VPCs 有 IPv6 地址 IPv4 或地址在两者之间路由流量。 AWS Transit Gateway VPCs 连接到单个 Transit Gateway 实例，该实例将组织的整个 AWS 路由配置整合到一个地方。

有关更多信息，请参阅构建可扩展且安全的多 VPC AWS 网络基础设施 AWS 白皮书。

> **注意**
>
> 要大规模创建和管理多 VPC AWS 网络基础设施，最佳实践是使用 AWS Transit Gateway。

在 VPC 对等连接和AWS Transit Gateway之间做出选择时的关键注意事项

VPC 对等连接

- 每个 VPC 之间的流量在每个 VPC 之间单独管理。
- VPC 对等连接不支持传递的路由。每个 VPC 之间都需要直接 VPC 对等连接，且必须相互之间进行通信。

AWS Transit Gateway

- 每个 VPC 之间的流量通过该 AWS Transit Gateway 服务进行管理，该服务充当连接每个 VPC 的集中中心。
- AWS Transit Gateway 支持传递路由。流量使用路由表在所有连接的网络之间进行路由。

后续步骤

有关多 VPC 管理的更多信息，请参阅 Amazon VPC 用户指南中的与其他账户共享 VPC。

资源

- 使用 VPC 流日志记录 IP 流量（Amazon VPC 用户指南）
- 使用 CloudWatch 见解分析日志（适用于 A pache 的亚马逊托管服务 Flink 开发者指南）
- 使用安全组控制访问权限（Amazon RDS 用户指南）

文档历史记录

下表介绍了本指南的一些重要更改。如果您希望收到有关未来更新的通知，可以订阅 RSS 源。

变更	说明	日期
初次发布	—	2022 年 11 月 2 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。