在 AWS 雲端中保護 VPC 的傳出網路流量

AWS 方案指引

AWS 方案指引: 在 AWS 雲端中保護 VPC 的傳出網路流量

Table of Contents

保護 VPC 在 AWS 雲端中的傳出網路流量

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

2022 年 11 月 (文件歷史記錄)

本指南涵蓋使用 Amazon Virtual Private Cloud (Amazon VPC) 時保護和監控輸出網路流量的最佳實務和工具。它也說明可協助您監控來自彈性網路介面和 AWS 雲端中虛擬私有雲端 (VPCs) 傳出網路流量 AWS 的工具。

> **注意**
>
> 本指南不涵蓋可與 整合的第三方工具 AWS ，以提供額外的安全層。它也假設只有雲端架構。本指南不適用於混合式架構。

本指南概述了以下最佳實務：

- 透過分析現有流量模式來確定 VPC 的安全性需求
- 使用安全群組來限制 VPC 的輸出流量
- 使用 AWS Network Firewall 和 DNS 主機名稱來限制 VPC 的傳出流量
- 使用 VPC 端點存取 AWS 資源
- 使用 在內部應用程式之間建立私有連線 AWS PrivateLink
- 跨 VPCs 和 AWS 區域 使用 VPC 對等互連或 進行通訊 AWS Transit Gateway

> **注意**
>
> 為了獲得最佳的安全狀態，您也可以透過專用路徑將輸出流量傳送至篩選工具，例如防火牆設備。

目標業務成果

本指南可協助您執行以下操作：

1. 控制和監控 VPC 的輸出網路流量。

2. 請確定 AWS 資源之間的流量通過 AWS 由骨幹網路控制的安全的私有路由。
3. 實作 AWS 工具來持續監控傳出網路流量，並停止對未核准端點的請求。

確定 VPC 的安全要求

> **重要**
>
> 最佳實務是在測試環境中設計和測試 VPC 的輸出流量安全架構。在開發環境中測試架構變更可降低產生意外系統行為的風險。

在變更網路輸出流量模式之前，了解應用程式按預期運作所需的流量模式非常重要。此資訊可協助您識別在重新架構網路時允許的流量模式，以及拒絕的流量模式。

若要分析 VPC 的現有輸出流量模式，請先開啟 VPC 流程日誌。然後，使用測試環境在各種使用案例中執行應用程式，並分析流程日誌中的模擬流量。

VPC 流量日誌會記錄 VPC 的輸入和輸出 IP 流量。然後，Amazon VPC 會將日誌傳送至 Amazon Simple Storage Service (Amazon S3) 或 Amazon CloudWatch。可以使用下列任一工具來檢視和分析日誌：

- (對於 Amazon S3) Amazon Athena
- (對於 CloudWatch) CloudWatch Logs Insights

如需更多資訊和查詢範例，請參閱下列內容：

- 查詢 Amazon VPC 流程日誌 (Amazon Athena 使用者指南)
- 如何搭配使用 CloudWatch Logs Insights 查詢與 VPC 流程日誌？ (AWS 知識中心)
- CloudWatch Logs Insights 查詢語法 (Amazon CloudWatch Logs 使用者指南)

如需有關 VPC 流程日誌擷取之資訊類型的詳細資訊，請參閱《Amazon VPC 使用者指南》中的流程日誌記錄範例。

> **注意**
>
> VPC 流程日誌不會擷取應用程式層 (第 7 層) 資訊，例如 DNS 主機名稱。如果您的安全要求需要對應用程式層資料進行分析，可以部署 AWS Network Firewall 來擷取所需的詳細資訊。如需詳細資訊，請參閱本指南中使用 AWS Network Firewall 和 DNS 主機名稱限制 VPC 的傳出流量一節。

使用 VPC 流量日誌時分析 VPC 輸出流量的最佳實務

使用 Amazon Athena 或 CloudWatch Logs Insights 查詢來分析 VPC 流程日誌時，請務必執行以下操作：

- 識別和分析流經與應用程式所使用資源附接的彈性網路介面的輸入和輸出流量。
- 識別和分析流經與 NAT 閘道附接的網路介面的應用程式流量。
- 請確定擷取網路介面的所有輸出流量，方法是將查詢中的來源地址設為網路介面的私有 IP 地址。
- 撰寫查詢，僅專注於非預期的流量模式。(例如，如果應用程式與第三方實體 (例如 HTTPS API 端點) 進行通訊，則您可以建構查詢以便不包含這些實體。)
- 調查每個連接埠和目的地 IP 地址的有效性。(例如，對於堡壘主機或使用 SSH 從 Git 中複製儲存庫的主機，輸出目的地連接埠 22 可能是正常的。)

> **注意**
>
> 如果您是第一次使用 Amazon Athena，請務必設定查詢結果位置。如需指示，請參閱《Amazon Athena 使用者指南》中的使用 Athena 主控台指定查詢結果位置。

Amazon Athena 查詢範例

從特定網路介面傳回輸出管理流量的 Athena 查詢範例

下列 Athena 查詢會從 IP 地址為 10.100.0.10 的網路介面傳回前 200 行輸出管理流量：

```
SELECT * FROM "<vpc_flow_logs_table_name>"

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

LIMIT 200;
```

輸出範例

#	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
位元組	5445
start	1659310200
end	1659310225
動作	ACCEPT
log_status	OK
date	2022-07-16

> **注意**
>
> 此模式中的輸出為了演示目的已格式化，在您的系統上可能會有所不同。

Athena 查詢範例會傳回從特定 VPC 中接收最多流量的外部 IP 地址

下列 Athena 查詢會傳回從 VPC (CIDR 區塊以 '10.32' 開頭) 中接收最多輸出流量的外部 IP 地址和連接埠：

```
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;
```

輸出範例

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

從特定 VPC 中傳回被拒絕的輸出流量的 Athena 查詢範例

下列 Athena 查詢會從 VPC (CIDR 區塊以 '10.32' 開頭) 中傳回被拒絕的輸出流量：

```
SELECT *

FROM "<vpc_flow_logs_table_name>"

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

輸出範例

#	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
位元組	5445
start	1659310200
end	1659310225
動作	REJECT
log_status	OK
date	2022-07-16

> **注意**
>
> 此模式中的輸出為了演示目的已格式化，在您的系統上可能會有所不同。

如需有關如何解譯 Athena 查詢結果的詳細資訊，請參閱《Amazon VPC 使用者指南》中的流量日誌記錄。

CloudWatch Logs Insights 查詢範例

從特定網路介面傳回輸出管理流量的 CloudWatch Logs Insights 查詢範例

下列 CloudWatch Logs Insights 查詢會從 IP 地址為 10.100.0.10 的網路介面傳回前 200 個輸出管理流量結果：

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

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

| filter srcAddr = '10.100.0.10'

| filter dstPort < 1024

| limit 200
```

輸出範例

欄位	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>
動作	ACCEPT
位元組	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
入門	1659310200
version	2

CloudWatch Logs Insights 查詢範例會傳回從特定 VPC 中接收最多流量的外部 IP 地址

下列 CloudWatch Logs Insights 查詢會傳回從 VPC (CIDR 區塊以 '10.32' 開頭) 中接收最多輸出流量的外部 IP 地址和連接埠：

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

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

| filter dstAddr not like '10.32'

| order by count desc

| limit 200
```

輸出範例

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

從特定 VPC 中傳回被拒絕的輸出流量的 CloudWatch Logs Insights 查詢範例

下列 CloudWatch Logs Insights 查詢會從 VPC (CIDR 區塊以 '10.32' 開頭) 中傳回被拒絕的輸出流量：

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

| fields @timestamp, @message
```

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

輸出範例

欄位	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>
動作	REJECT
位元組	43
dstAddr	10.10.2.222
dstPort	11211
end	1666990966
interfaceId	'eni-0123456789000000'
logStatus	OK
packets	1
protocol	17
srcAddr	185.x.x.x
srcPort	55116

入門	1666990939
version	2

限制 VPC 的輸出流量

使用安全群組來限制 VPC 的輸出流量

評估架構的輸出流量需求後，請開始修改 VPC 的安全群組規則，以符合組織的安全需求。請務必將所有必要的連接埠、通訊協定和目標 IP 地址新增至安全群組的允許清單。

如需相關說明，請參閱 Amazon VPC 使用者指南中的使用安全群組控制流向資源的流量。

> **Important (重要)**
>
> 在測試環境中更新 VPC 的安全群組規則後，務必確認您的應用程式仍如預期般運作。如需詳細資訊，請參閱本指南的使用 VPC 流量日誌時分析 VPC 輸出流量的最佳實務一節。

特定 AWS 服務的關鍵安全群組考量事項

Amazon Elastic Compute Cloud (Amazon EC2)

建立 VPC 時，會附帶一個允許所有輸出流量的預設安全群組。除非您建立自己的自訂安全群組，否則 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體會使用此預設安全群組。

> **Important (重要)**
>
> 為了降低 Amazon EC2 執行個體無意中使用預設安全群組的風險，請移除群組的所有輸出規則。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中使用安全群組規則一節中的刪除安全群組規則。

Amazon Relational Database Service (Amazon RDS)

除非資料庫充當用戶端，否則可移除 Amazon RDS DB 執行個體的所有輸出安全群組規則。如需詳細資訊，請參閱《Amazon RDS 使用者指南》中的 VPC 安全群組概觀。

Amazon ElastiCache

除非執行個體充當用戶端，否則可以移除 Amazon ElastiCache (Redis OSS) 和 Amazon ElastiCache (Memcached) 執行個體的所有傳出安全群組規則。如需詳細資訊，請參閱下列內容：

- 安全群組：EC2-Classic (Amazon ElastiCache (Redis OSS) 使用者指南)
- 了解 ElastiCache 和 Amazon VPCs(Amazon ElastiCache (Memcached) 使用者指南)

使用 AWS Network Firewall 和 DNS 主機名稱限制 VPC 的傳出流量

當應用程式使用動態 IP 地址時，最佳實務是使用 DNS 主機名稱而非 IP 地址來篩選其 VPC 的輸出流量。例如，如果應用程式正在使用 Application Load Balancer，則應用程式的關聯 IP 地址將會變更，因為節點會不斷擴展。在這種情況下，使用 DNS 主機名稱來篩選輸出網路流量比使用靜態 IP 地址更安全。

可以使用 AWS Network Firewall 將 VPC 的輸出網際網路存取限制到由 HTTPS 流量中的伺服器名稱指示 (SNI) 提供的一組主機名稱。

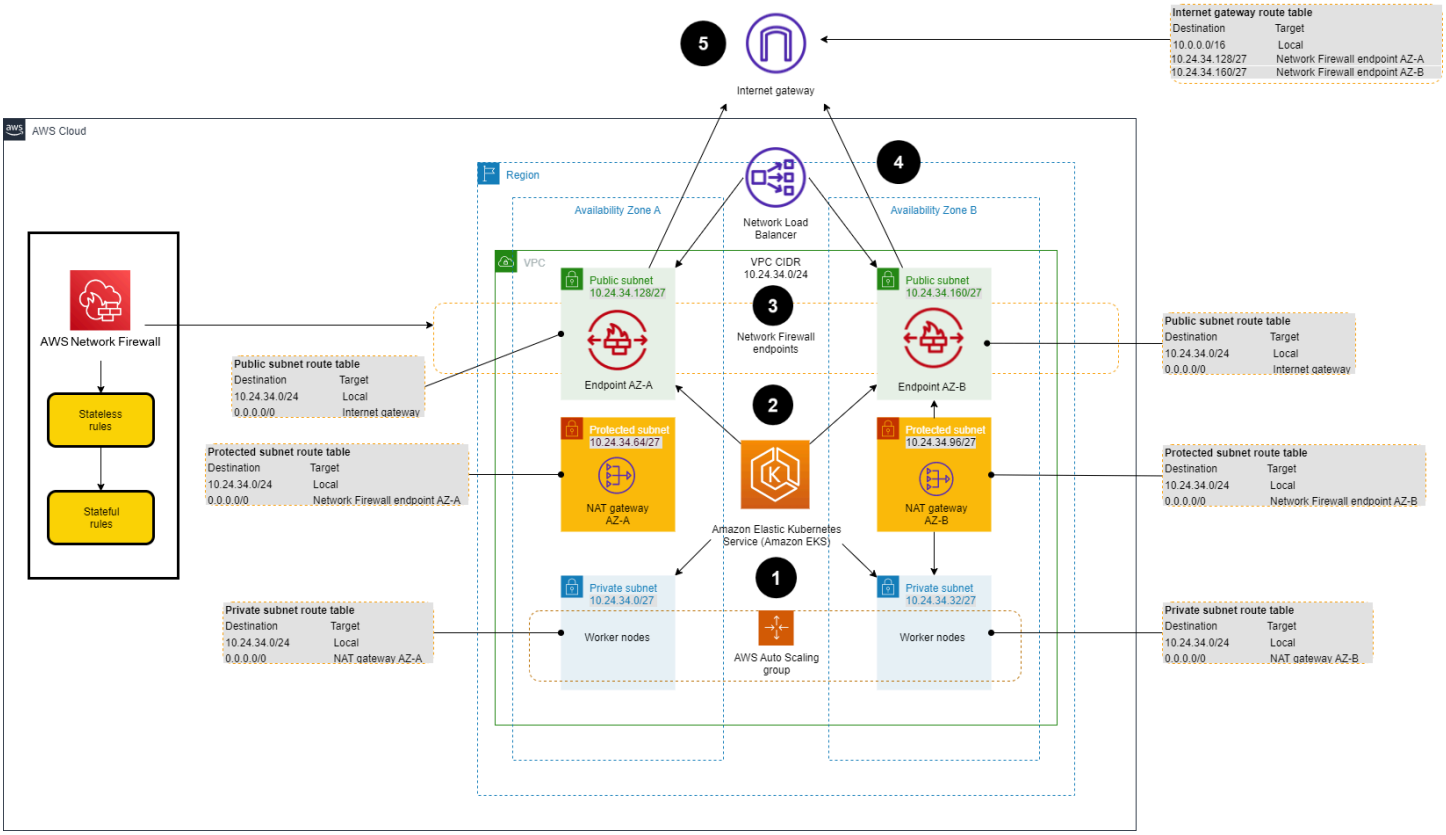
如需詳細資訊和網路防火牆政策規則範例，請參閱《AWS Network Firewall 開發人員指南》中的域篩選。如需詳細指示，請參閱下列 AWS 方案指引 (APG) 模式：使用網路防火牆從輸出流量的伺服器名稱指示 (SNI) 中擷取 DNS 域名稱。

> **注意**
>
> SNI 是 TLS 的延伸，可在流量中保持未加密狀態。這表示用戶端嘗試透過 HTTPS 存取的目的地主機名稱。

> **Important (重要)**
>
> 在測試環境中更新網路防火牆的帶狀態規則之後，請確定應用程式仍如預期般運作。請確定 SNI 提供的必要 DNS 域名未被阻止。

架構範例

下圖顯示使用 DNS 主機名稱 AWS Network Firewall 篩選 VPC 傳出流量的範例架構：



該圖顯示以下工作流程：

1. 輸出請求源自私有子網路，並傳送至受保護子網路中的 NAT 閘道。
2. NAT 閘道收到的 HTTPS 流量會路由到公有子網路中的 AWS Network Firewall 端點。
3. AWS Network Firewall 會檢查請求，並套用設定的防火牆政策規則，以接受或拒絕傳遞至網際網路閘道的請求。
4. 核准的輸出請求會傳送至網際網路閘道。
5. 來自網際網路閘道的核准流量會傳送至網際網路，以存取預期的 URL (由非加密 HTTPS 標頭中的 SNI 提供)。

存取 AWS 資源

VPC 端點可在 VPC 與支援的 AWS 服務之間提供私有連線，而不需要網際網路閘道或 NAT 閘道。例如，可以使用 VPC 端點將 VPC 連線至 Amazon Simple Storage Service (Amazon S3) 或 Amazon Elastic Container Registry (Amazon ECR)。

Amazon VPC 提供三種類型的 VPC 端點：

- 介面端點將 VPCs 連接到 支援的 Amazon VPC 服務 AWS PrivateLink。
- 閘道端點專門為 Amazon S3 和 Amazon DynamoDB 提供可靠的連線能力。
- 閘道負載平衡器端點將 VPC 連線到在閘道負載平衡器後方託管的自訂應用程式。

如需支援的服務清單，請參閱 Amazon VPC 文件中與 AWS PrivateLink整合的AWS 服務。

> **注意**
>
> Gateway Load Balancer 端點在私下與應用程式 VPC 或 AWS 帳戶以外的使用者共用應用程式時很有幫助。如需詳細資訊，請參閱本指南的在內部應用程式之間建立私有連線一節。

在內部應用程式之間建立私有連線

雲端型應用程式的端點可以使用 在 AWS 雲端上私下共用 AWS PrivateLink。如需詳細資訊和範例架構，請參閱 AWS PrivateLink 文件。

如需更多架構範例，請參閱下列 AWS 規範性指引模式：

- 使用 AWS PrivateLink 和 Network Load Balancer 在 Amazon ECS 上私下存取容器應用程式
- 使用 和 Network Load Balancer AWS FargateAWS PrivateLink在 Amazon ECS 上私下存取容器應用程式
- 使用 AWS PrivateLink 和 Network Load Balancer 在 Amazon EKS 上私下存取容器應用程式

跨 VPCs和 進行通訊 AWS 區域

多 VPC 基礎設施可協助組織細分工作負載並擴大其覆蓋範圍。當資源需要與不同 VPCs 和 AWS 帳戶中 AWS 的服務通訊時 AWS 區域，這種類型的架構也會產生挑戰。

若要在兩個 VPC 之間建立連線，可以使用 VPC 對等互連或者 AWS Transit Gateway。VPC 對等互連是兩個 VPCs 之間的網路連線，這些 VPC 使用私有 IPv4 或 IPv6 地址路由流量。 會將 VPCs AWS Transit Gateway 連接到單一 Transit Gateway 執行個體，將組織的整個 AWS 路由組態合併在一個位置。

如需詳細資訊，請參閱建置可擴展且安全的多 VPC AWS 網路基礎設施 AWS 白皮書。

> **注意**
>
> 若要大規模建立和管理多 VPC AWS 網路基礎設施，最佳實務是使用 AWS Transit Gateway。

在 VPC 對等互連與AWS Transit Gateway之間進行選擇的重要考量事項

VPC 對等互連

- 每個 VPC 之間的流量在每個 VPC 之間單獨管理。
- VPC 對等互連不支援傳遞路由。必須彼此通訊的每個 VPC 之間需要直接的 VPC 對等互連。

AWS Transit Gateway

- 每個 VPC 之間的流量是透過 AWS Transit Gateway 服務管理，該服務可做為連接每個 VPC 的集中式中樞。
- AWS Transit Gateway 支援暫時性路由。透過使用路由表，在所有連接的網路之間路由流量。

後續步驟

如需有關多 VPC 管理的詳細資訊，請參閱《Amazon VPC 使用者指南》中的與其他帳戶共用 VPC。

Resources

- 使用 VPC 流量日誌來記錄 IP 流量 (Amazon VPC 使用者指南)
- 利用 CloudWatch Insights 分析日誌 (Amazon Managed Service for Apache Flink 開發人員指南)
- 使用安全群組控制存取 (Amazon RDS 使用者指南)

文件歷史紀錄

下表描述了本指南的重大變更。如果您想收到有關未來更新的通知，可以訂閱 RSS 摘要。

變更	描述	日期
初次出版	—	2022 年 11 月 2 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。