亚马逊云科技

Security Day—云端IPS/IDS防护

Network Firewall 网络和应用边界防护

安全防护的主要需求

安全监控和威胁探测

数据保护

网络和应用防护

网络和应用防护面临的主要风险

拒绝服务攻击

- SYN floods
- Reflection attacks
- Web request floods

APP 漏洞

- SQL injection
- Cross-site scripting (XSS)
- OWASP Top 10
- Common vulnerabilities and exposures (CVE)

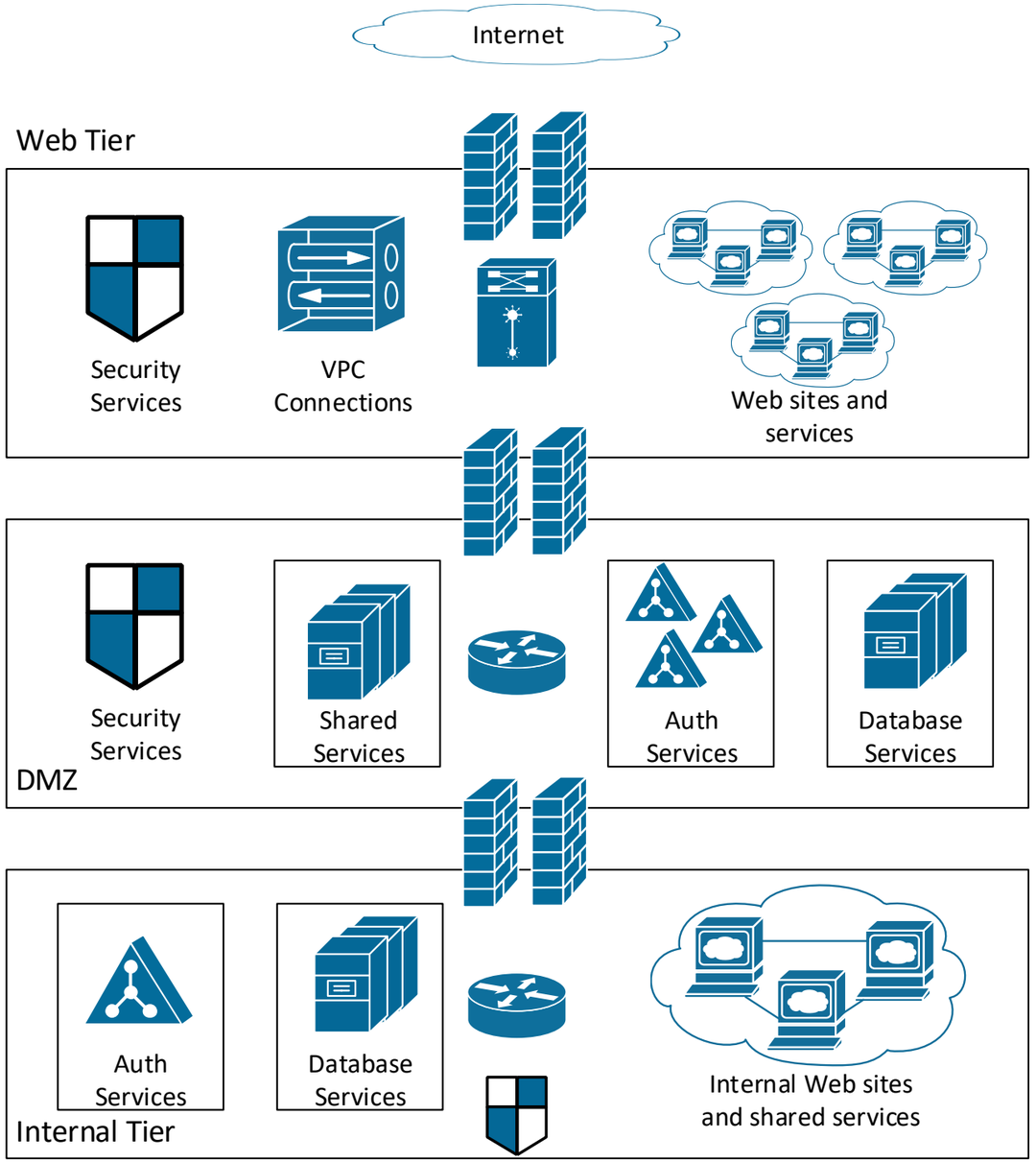
恶意机器人

- Crawlers
- Content scrapers
- Scanners and probes

传统边界防护架构

网络为中心的安全

- 边界路由器
- 防火墙（有状态/无状态）
- IPS/IDS
- 防DDOS
- IPSEC VPN/Remote Client VPN
- 目标域名过滤



网络和应用边界防护服务

Network Firewall

采用IPS、状态检查、URL过滤
、保护VPC

WAF

支持自定义规则、托管规则或从应用市场购买第三方规则保护WEB应用程序

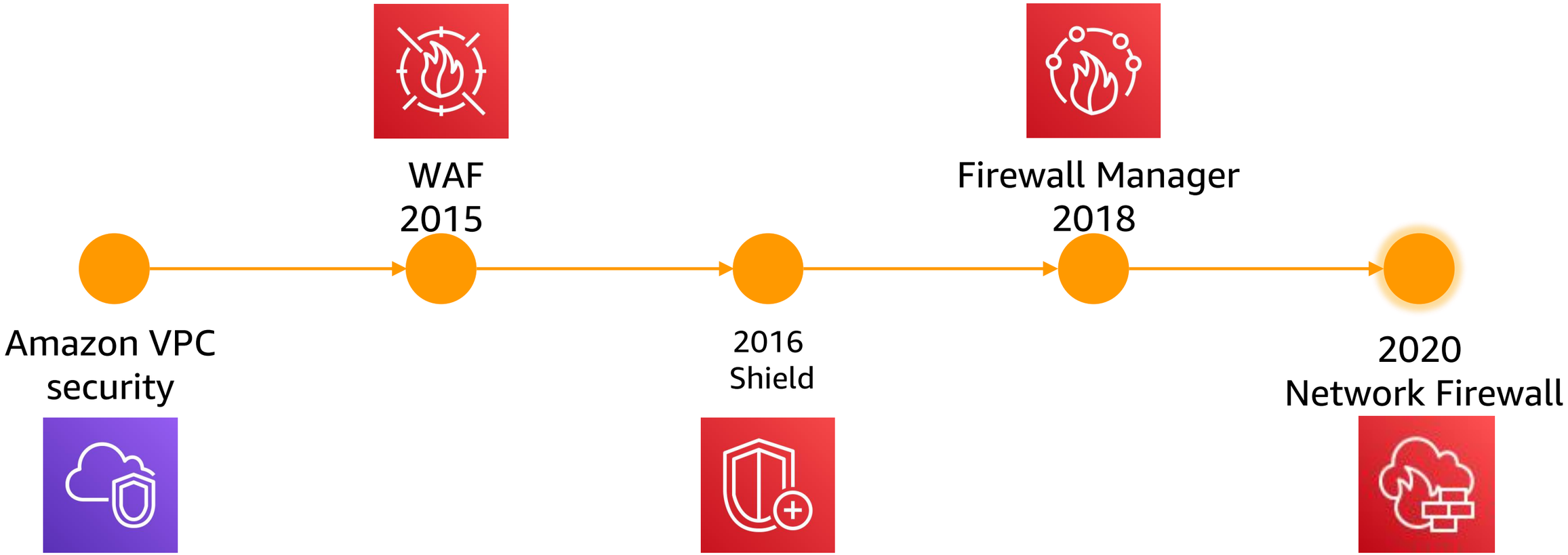
Shield Advanced*

防护DDOS攻击，漏洞暴漏，恶意程序（无需额外成本使用WAF和Firewall Mnager）

Firewall Manager

跨帐户和应用程序集中配置和管理安全规则

云端安全防护服务发展历程



Amazon Network Firewall 简介

VPC级别的防护罩（SG 实例级别，NACL 子网级别）

3-7层防火墙 （7层WAF，3-4层SG和NACL）

安全检测

VPC-to-VPC 流量

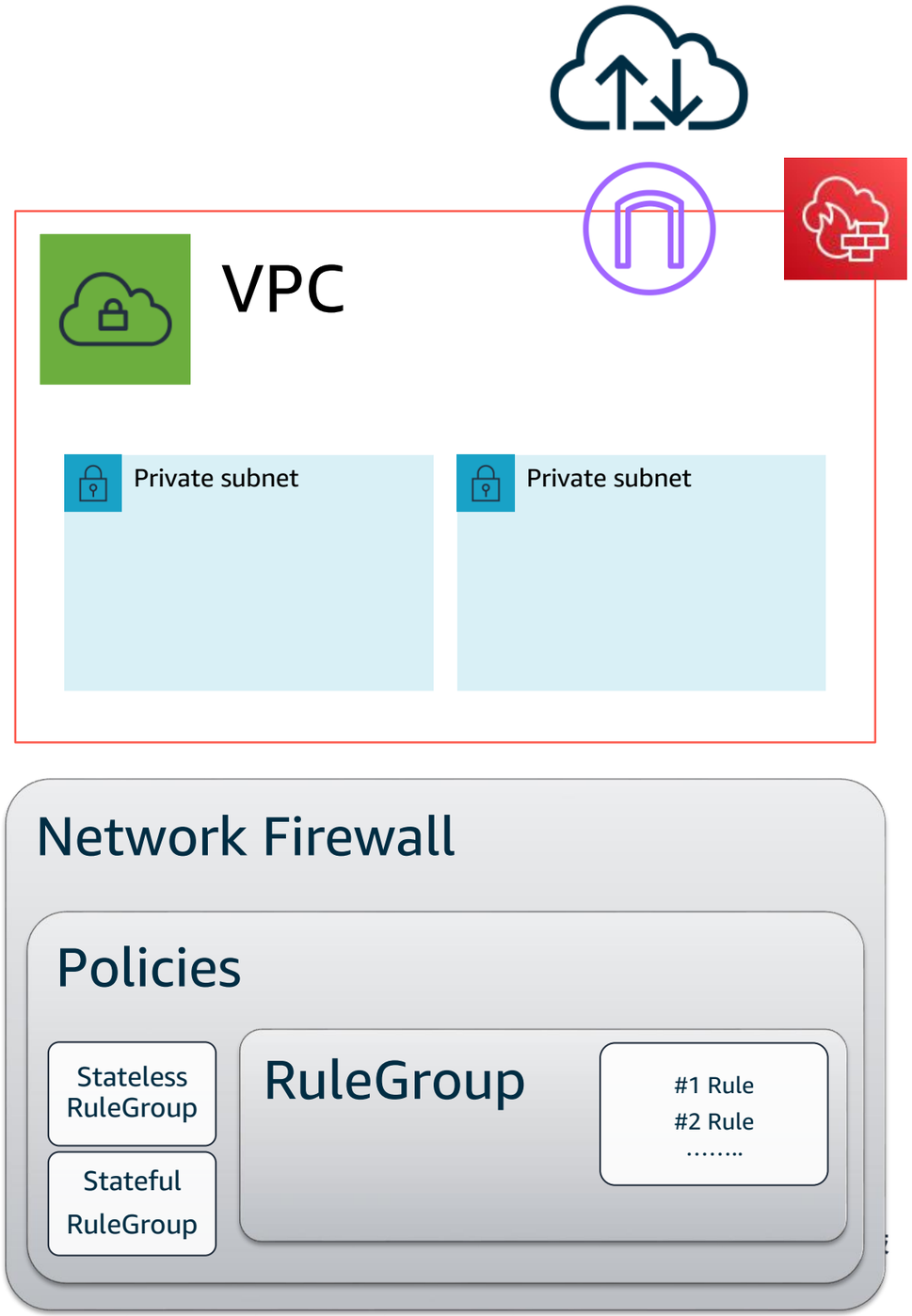
出互联网流量

来源于互联网流量

流经DX/VPN流量

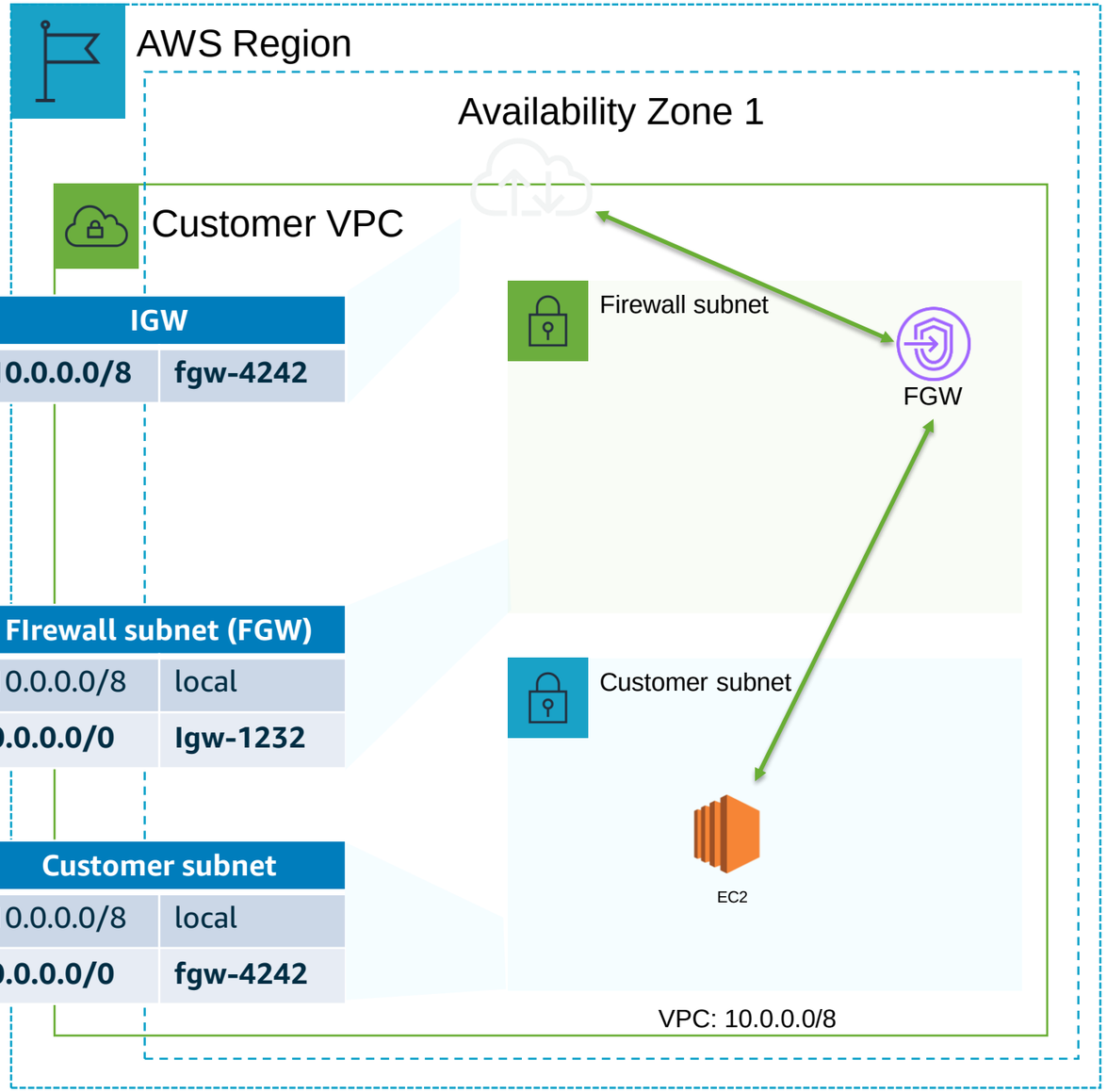
AWS Network Firewall组件

- 防火墙终端节点
- 策略 （1 policy per firewall）
- 规则组 （n RuleGroup per policy）



NetWork Firewall 工作原理

Network Firewall – 部署方式



防火墙作为VPC子网内的终端节点

必须存在于它自己的单独子网

不需要在多台防火墙之间进行负载均衡

是否可以跨多个AZ部署，每个AZ中出现一个端点

集成第三方合作伙伴

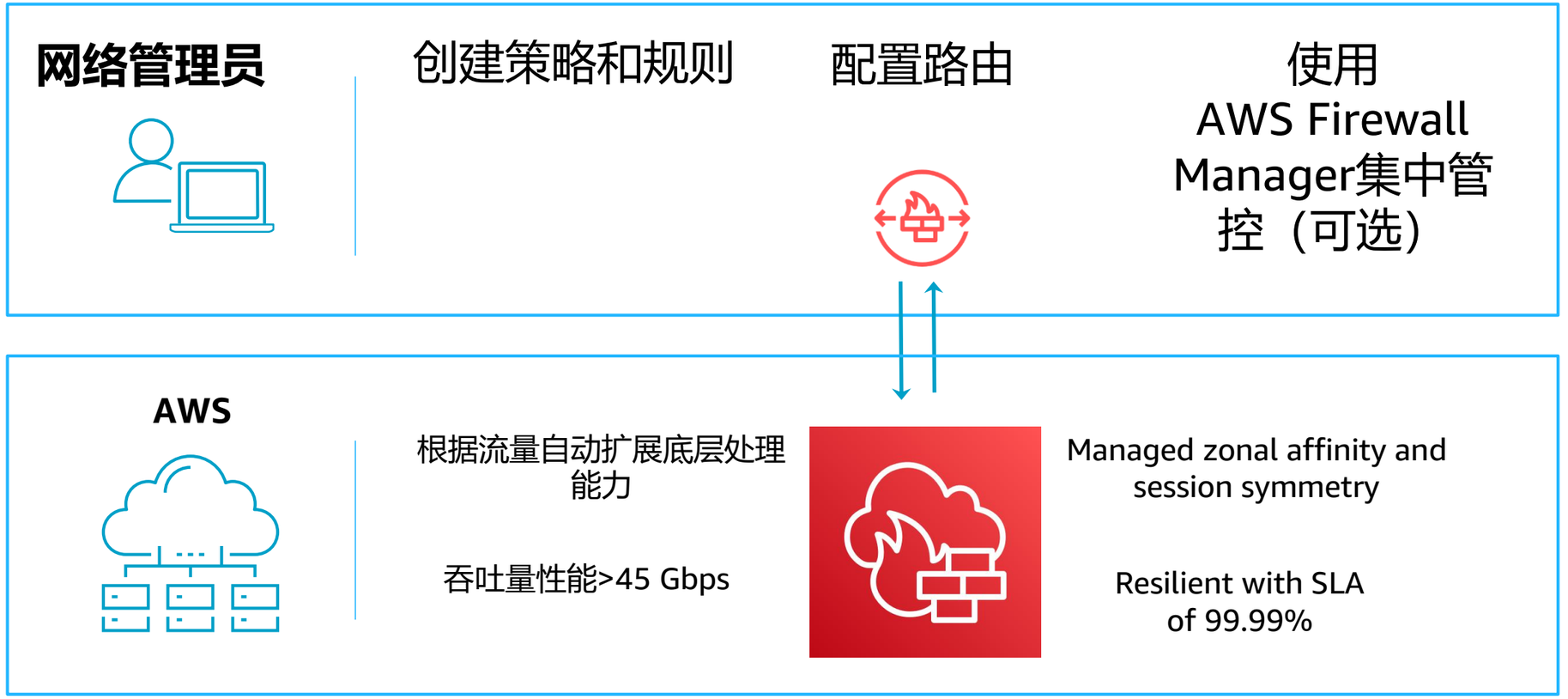
安全监控

威胁情报

策略管理

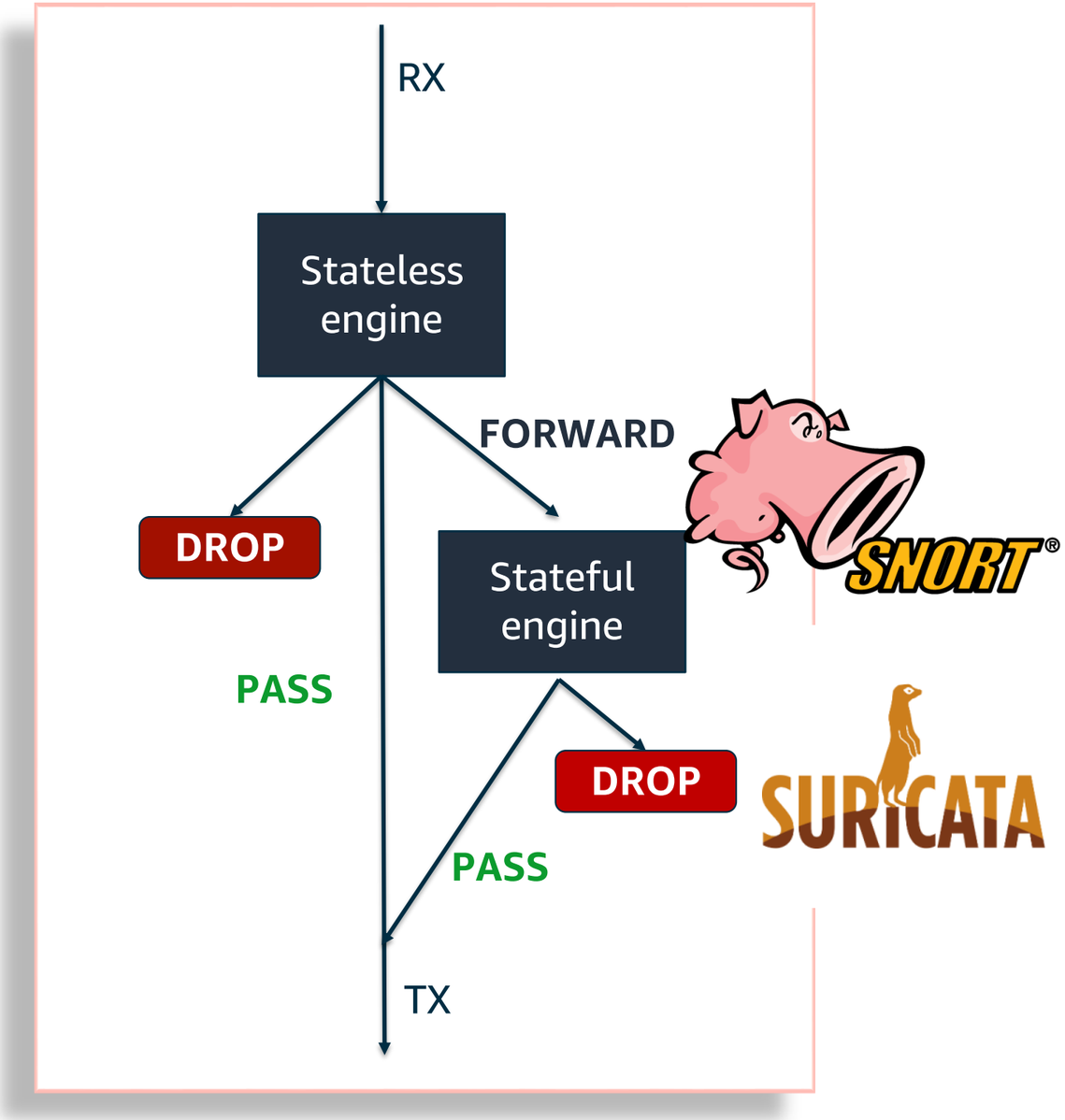
安全管理

Amazon Network Firewall 责任界面



处理流程

- 无状态引擎接收所有流量
- 无状态规则动作（规则优先级）：
  - Pass、Drop
  - Forward to 有状态规则
  - Custom Action
- 有状态规则动作（动作类型优先）：
  - Pass、Drop、Alert
- 支持双向流动



无状态规则组

无状态的规则匹配属性:

- 源IP和目的IP
- 端口 (i.e. SourcePorts and DestinationPorts)
- 协议
- TCP标志(i.e. Flags and Masks)

Rule Actions:

- Drop (aws:drop)
- Pass (aws:pass)
- Forward to stateful (aws:forward_to_sfe)
- Custom * (CustomAction)
    - 当前支持Cloudwatch metric

有状态规则组

有状态规则匹配属性:

- 5元组 (协议，源和目的IP，源和目的端口)
- 域名
- Snort或者Suricata脚本

Rule Actions:

- Drop (aws:drop)
- Pass (aws:pass)
- Alert

- pass http $HOME_NET any -> $EXTERNAL_NET any (http.host; dotprefix; content:".example.com"; endswith; msg:"Allowed HTTP domain"; priority:1; sid:102120; rev:1;)
- drop tcp $HOME_NET any <> $HOME_NET any (msg:"Blocked TCP that is not HTTP"; flow:established; app-layer-protocol:!http; sid:102121; rev:1;)
- drop ip $HOME_NET any <> $HOME_NET any (msg: "Block non-TCP traffic."; ip_proto:!TCP;sid:8; rev:1;)

注意：Domain Name filtering 集中部署模型中需要CLI设置HOME_NET，添加所有需过滤VPC CIDR

https://docs.aws.amazon.com/zh_cn/network-firewall/latest/developerguide/suricata-limitations-caveats.html
https://suricata.readthedocs.io/en/suricata-6.0.2/rules/meta.html

规则容量计算方式

网络防火墙使用容量设置来计算和管理其规则组和防火墙策略的处理要求。

规则组创建后不能更改容量，并且规则组中规则总容量不能超过规则组设定的容量。

创建规则组时需要预留一定容量冗余。

ALL 和 ANY 记1 容量

具有criteria规范的匹配设置的复杂性值等于设置中的规范数量。

例如，设置为UDP的协议规范和设置为10.0.0.0/24的源规范的值都是1。

协议为UDP, TCP为2，

源为10.0.0.0/24,10.0.1.0/24,10.0.2.0/24为3。

```
pass http $HOME_NET any -> any any (http.host; dotprefix; content:".example.com"; endswith; msg:"Allowed HTTP domain";
priority:1; sid:102120; rev:1;)
```

限制

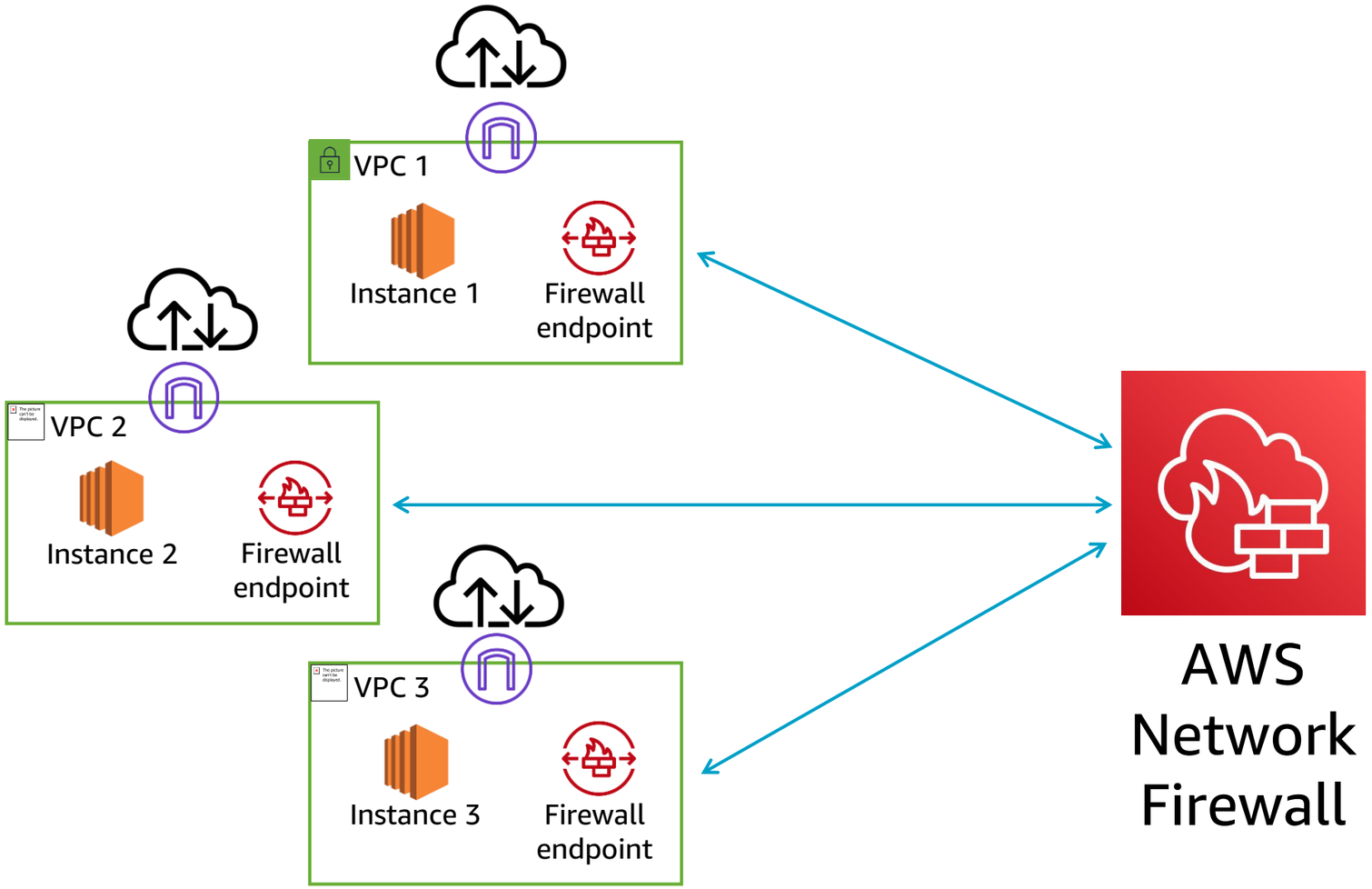
软限制

资源	默认限额（每账号每区域）
最大防火墙数量	5
最大防火墙策略	20
最大有状态规则组数量	50
最大无状态规则组数量	50

硬限制

资源	限额（每账号每区域）
规则组中与suricata兼容的规则字符串的最大大小(以字节为单位)。	1,000,000（1M）
有状态规则组最大容量。	30,000
每个防火墙策略中有状态规则组的最大数目。	10
每个防火墙策略中有状态规则最大数目。这是策略引用的所有规则组的总数。	30,000
最大无状态规则组容量。	10,000
每个防火墙策略中无状态规则组的最大数目。	10
每个防火墙策略中无状态规则的最大数目。这是策略引用的所有规则组的总数。	10,000
每个防火墙所需的防火墙策略数量。	1
可以使用同一防火墙策略的最大防火墙数。	1,000
可以使用同一规则组的最大防火墙策略数。	1,000

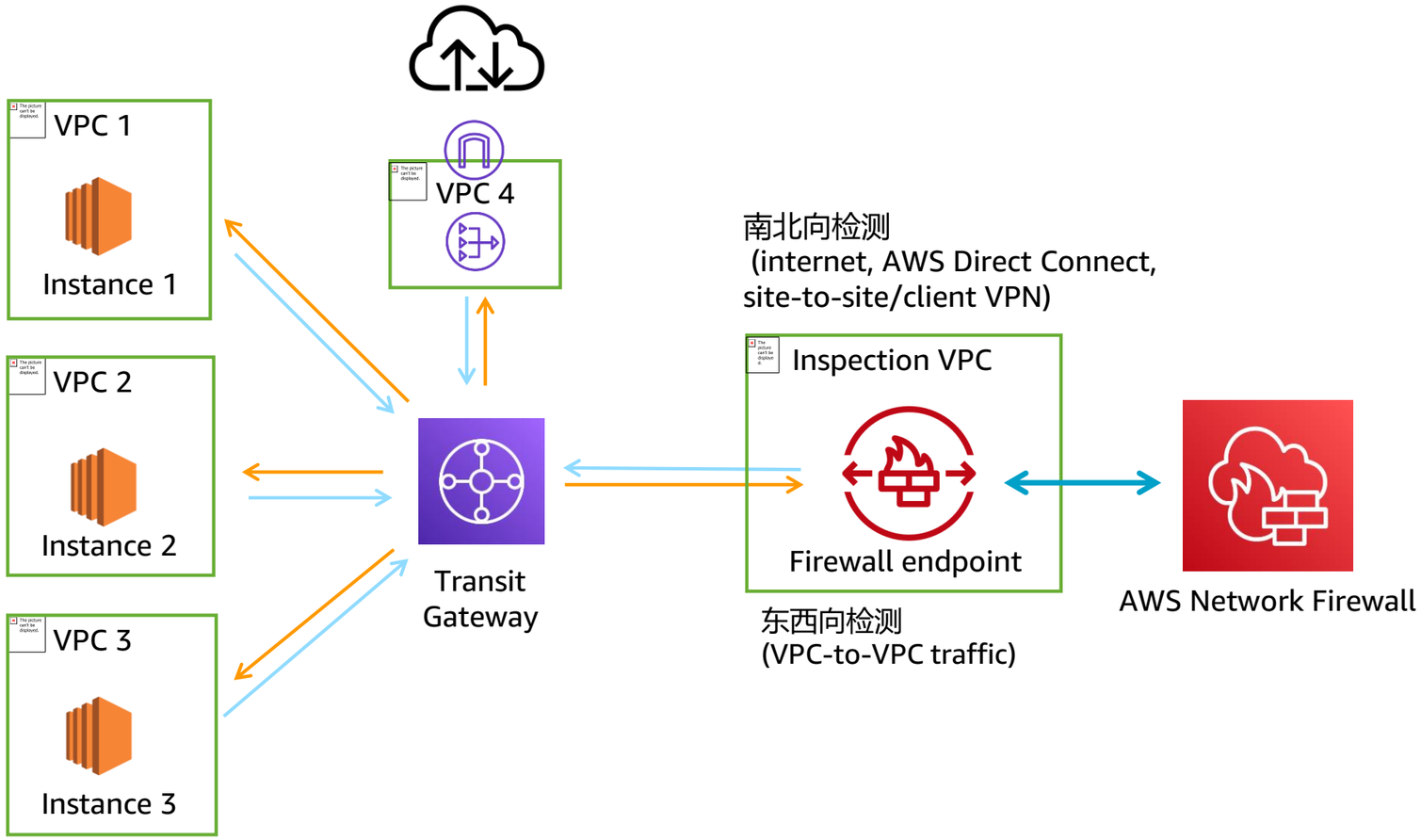
分布式部署模型



适用客户：

- 单体客户或分支具有独立管控权限的客户
- 多业务系统各自独立，具有单独互联网出口
- 要求具有托管的3-7层防火墙
- 要求VPC级别整体安全防护

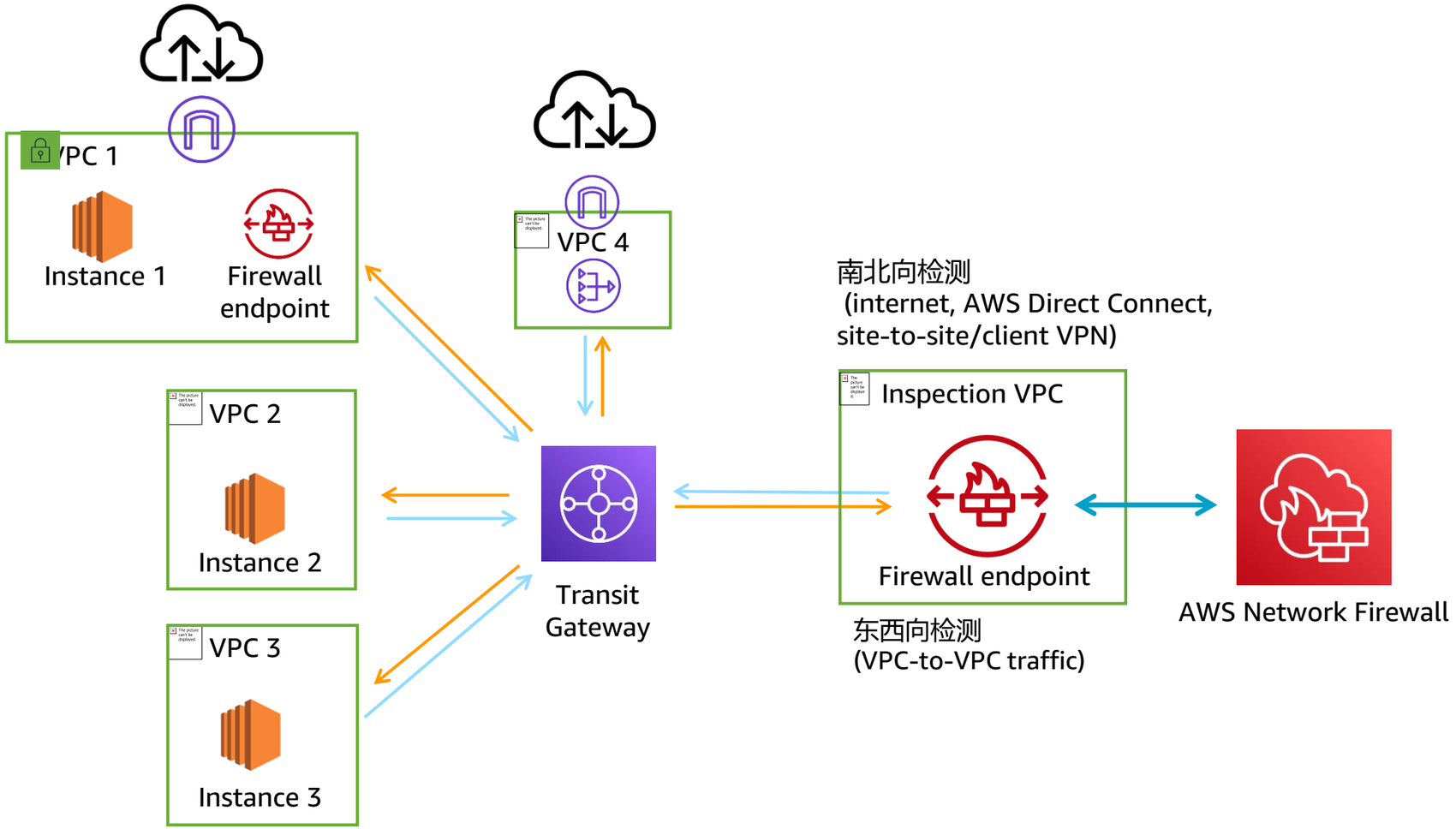
集中式部署模型



适用客户：

- 集团型客户，中央集权
- 统一网络出口，进行集中防护
- 不同业务域间需进行安全防护

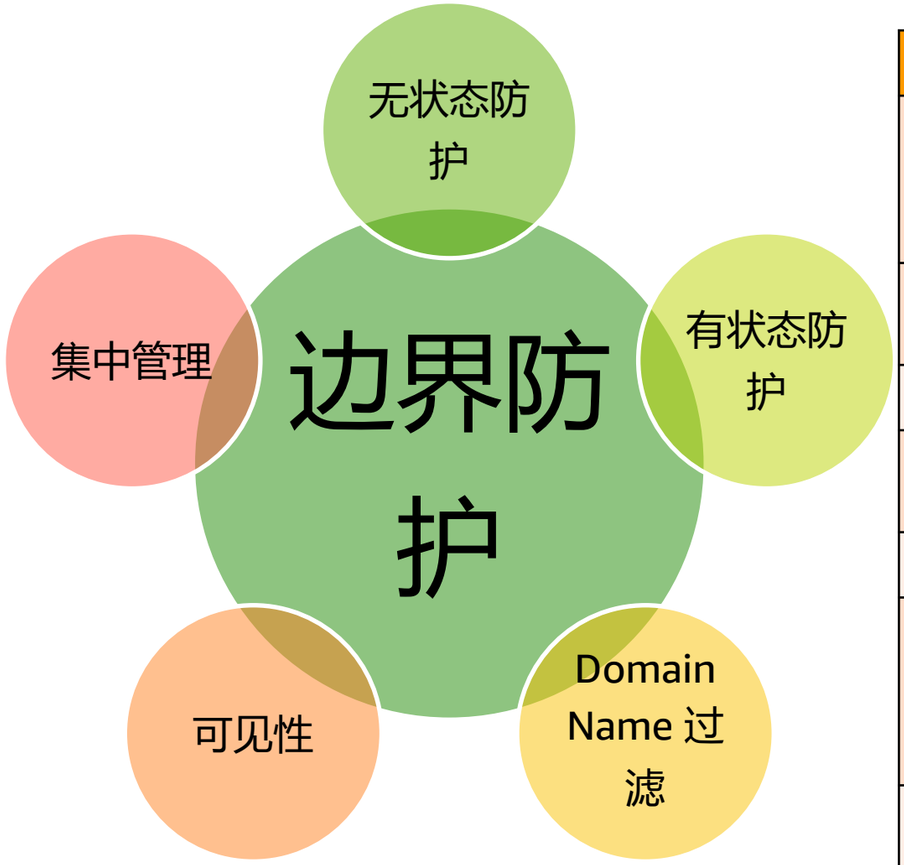
混合部署模型



适用客户：

- 集团型客户，中央集权
- 统一网络出口，进行集中防护
- 具有特殊业务独立网络出口
- 不同业务域间需进行安全隔离

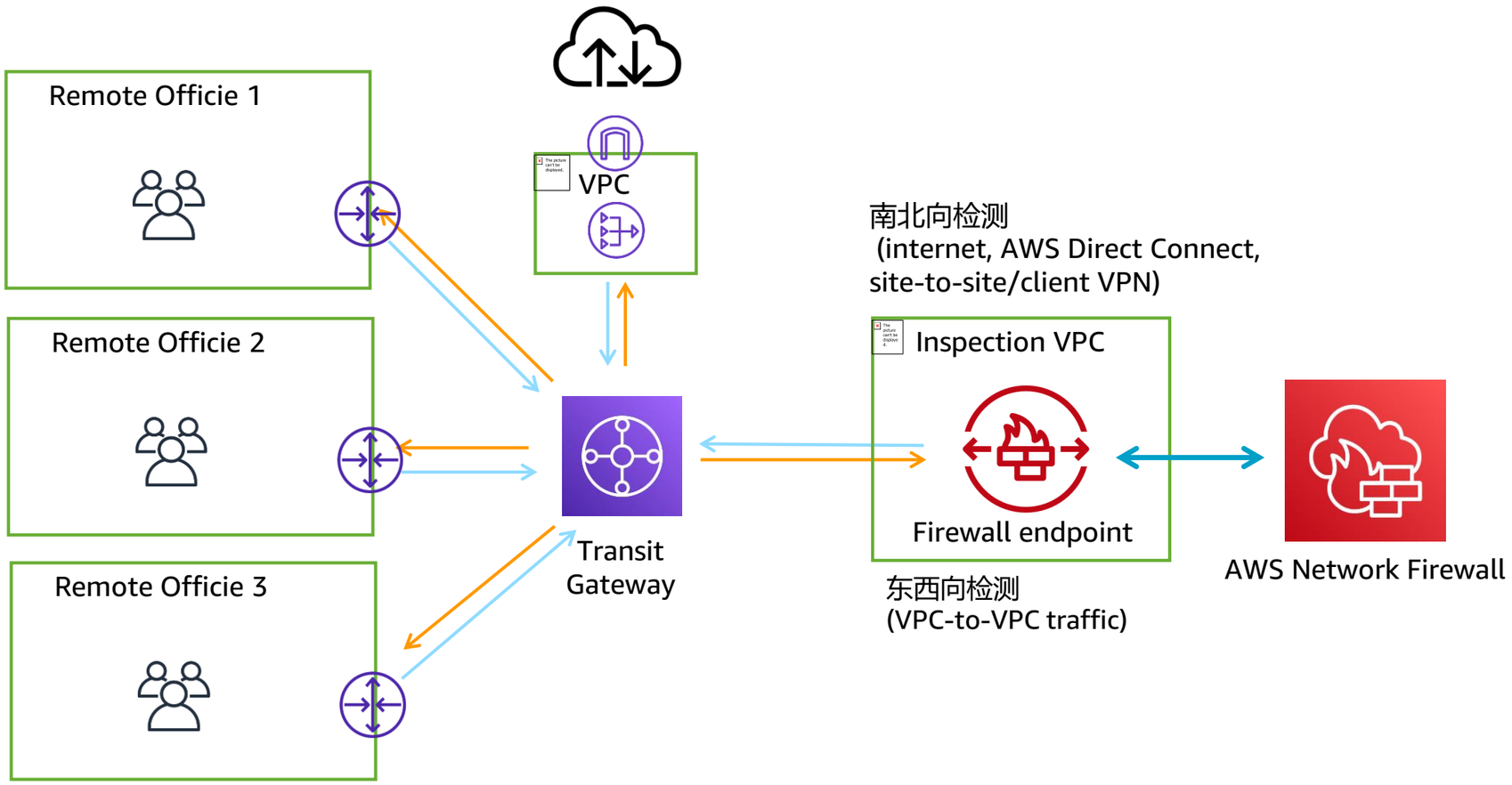
网络和应用防护的主要场景



功能	应用场景	部署模式	涉及服务
Domain Name过略	ERP/供应链/支付等访问第三方关联系统	分布式部署 集中式部署	NFW TGW+NFW
	上网行为管理	集中式部署	TGW+DX+NFW
无状态防护（类似NACL）	互联网边界防护	分布式部署 集中式部署	NFW TGW+NFW
	多业务VPC及本地数据中心之间防护	集中式部署	TGW+DX+NFW
有状态防护（IPS，类似SG）	互联网边界防护	分布式部署 集中式部署	NFW TGW+NFW
	多业务VPC及本地数据中心之间防护	集中式部署	TGW+DX+NFW
可见性和报告	统一监控，日志导出供进一步分析处理		CloudWatch Metric CloudWatch Logs S3 Kinesis Firehose
集中管理	统一配置管理		Firewall Manager
	现有方案集成		14家第三方集成
	分支机构边界防护	集中式部署	TGW+DX/VPN+NFW

https://quip-amazon.com/0YN0A34e8gt8/Untitled#FcU9CAkcn5Q Security Day Opps collection and tracking Quip

远程分支边界防护参考架构



适用客户：

- 拓展海外业务，并在当地设立分支办公室

要求：

- 具有专线或互联网接入链路
- 支持专线接入或IPSec VPN小型路由设备

优势：

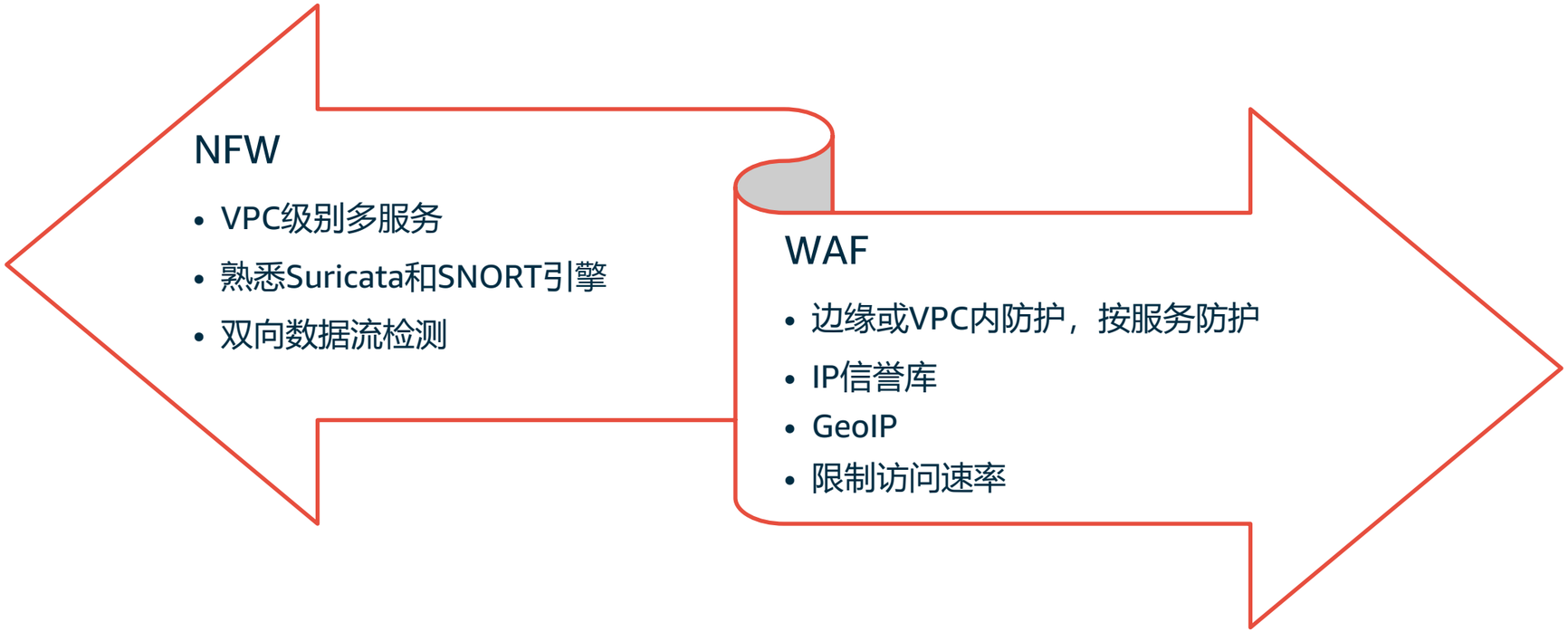
- 快速灵活，无需在当地配置专业IT人员
- 无需采购多种硬件设备及部署复杂架构
- 提供分支机构所需的3-7层安全防护
- 具有详尽的日志记录

部署模式选择

	分布式部署模型	集中式部署模型	联合部署模型
东西向: VPC间流量	不支持	支持	支持
南北向: VPC 出入互联网流量 VPC to Internet traffic flow	支持	支持	支持
南北向: VPC出入IDC流量（VPN/DX)	不支持	支持	支持
前提条件	专用的Network FireWall 子网	专用的防火墙VPC 和TGW	专用Network FireWall 子网/受保护VPC；专用的防火墙VPC 和TGW
集中管理	AWS Firewall Manager	单个Network Firewall	AWS Firewall Manager
源IP可见性	依赖于配置（与NAT Gateway相关）	Yes	依赖于配置（与NAT Gateway相关）
错误配置/故障爆炸半径	最小	中	低
成本	按NFW endpoint数量计算	TGW 计费（attachment数量+处理数据量） NFW endpoint	TGW 计费（attachment数量+处理数据量） NFW endpoints

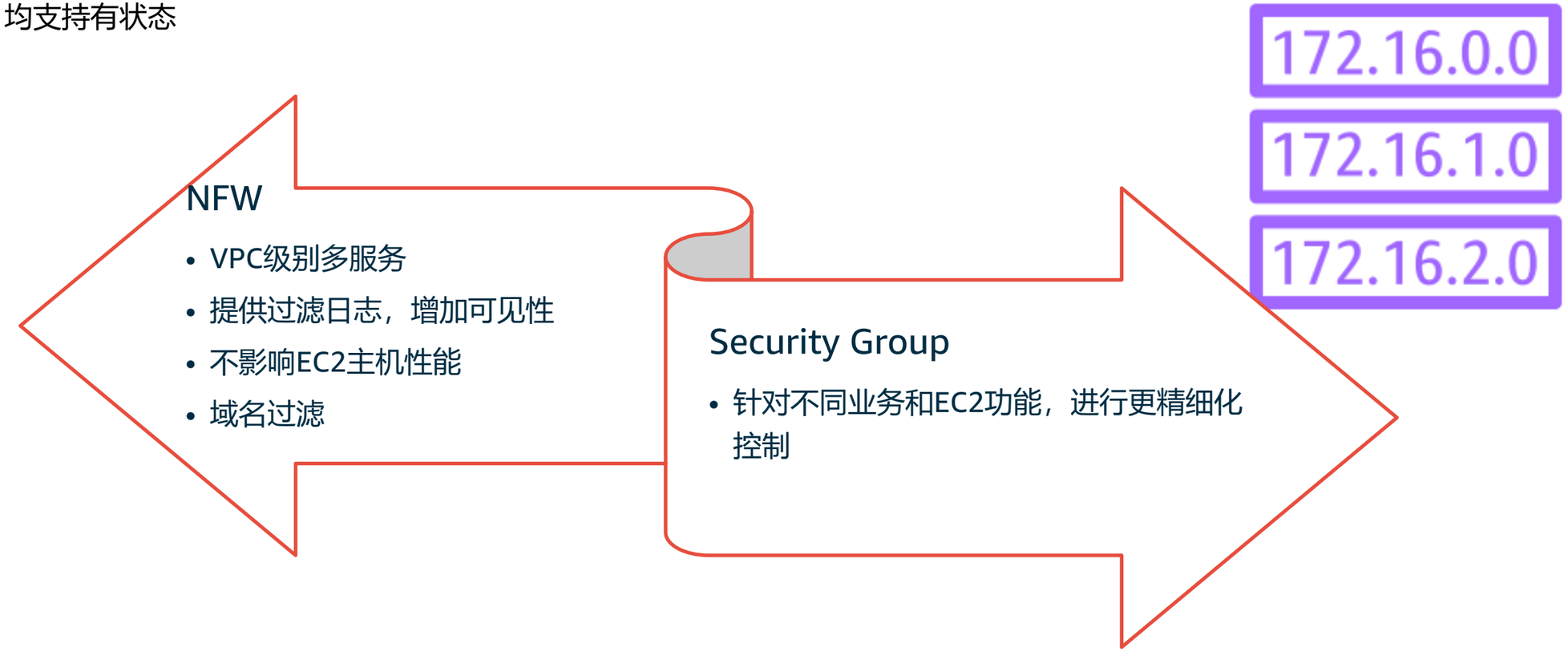
WAF VS Network Firewall

均支持7层

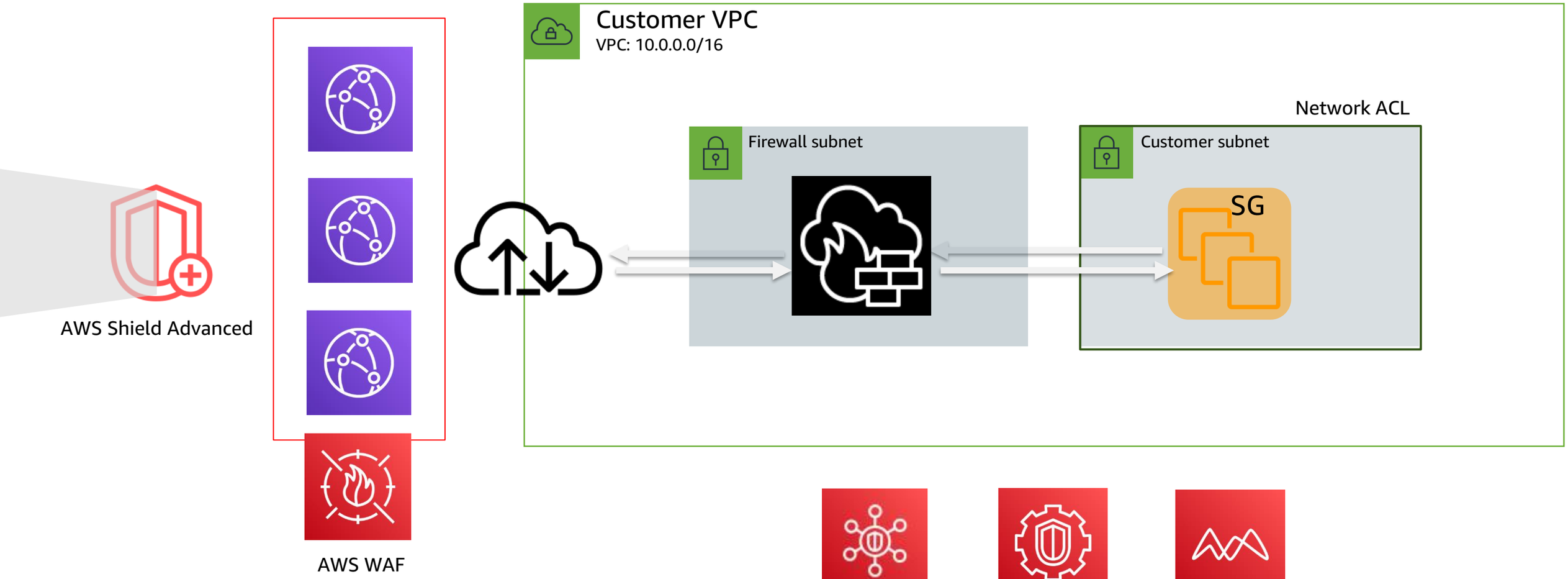


Amazon Network Firewall vs Security Groups

- 均支持有状态



构建纵深防御架构



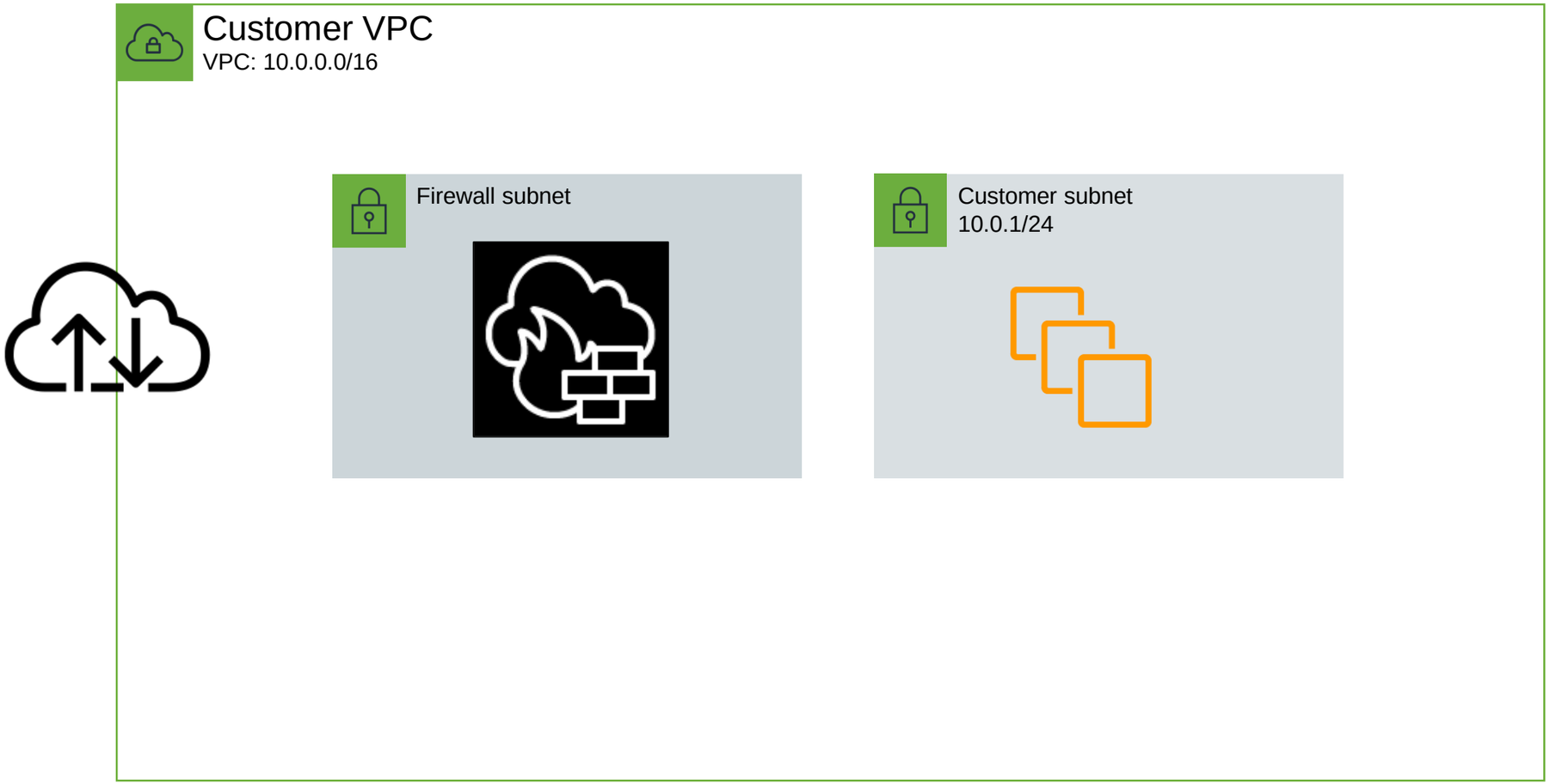
计费规则及可用Region

Resource Type	Price
网络防火墙终端节点小时费	$0.395/hr
网络防火墙流量处理费用	$0.065/GB
NAT网管费用	Use one hour & one GB of NAT gateway at no additional cost for every hour & GB charged for Network Firewall endpoints.

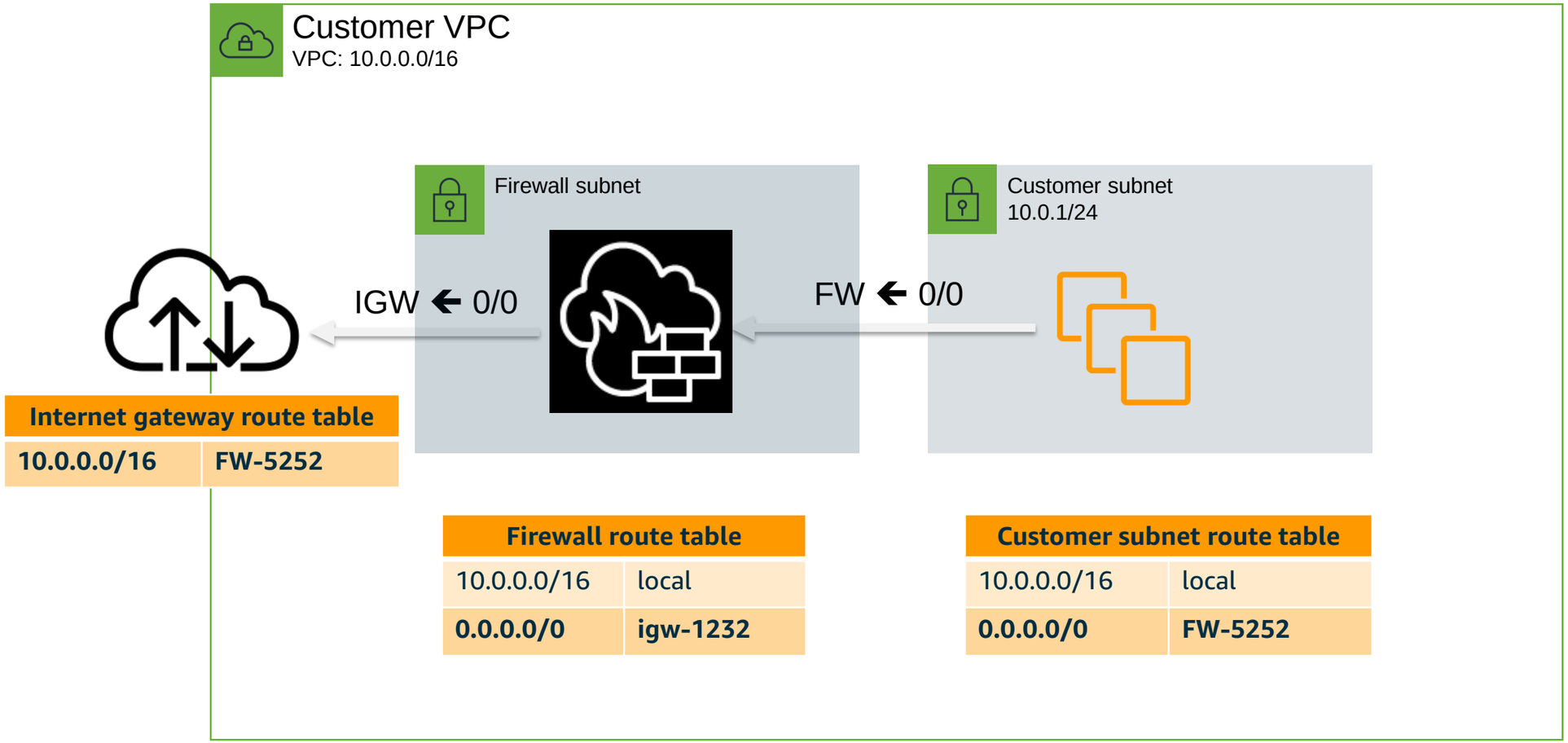
US East (N. Virginia)
US West (Oregon)
Europe (Ireland)
Asia Pacific (Sydney)

如何开始使用

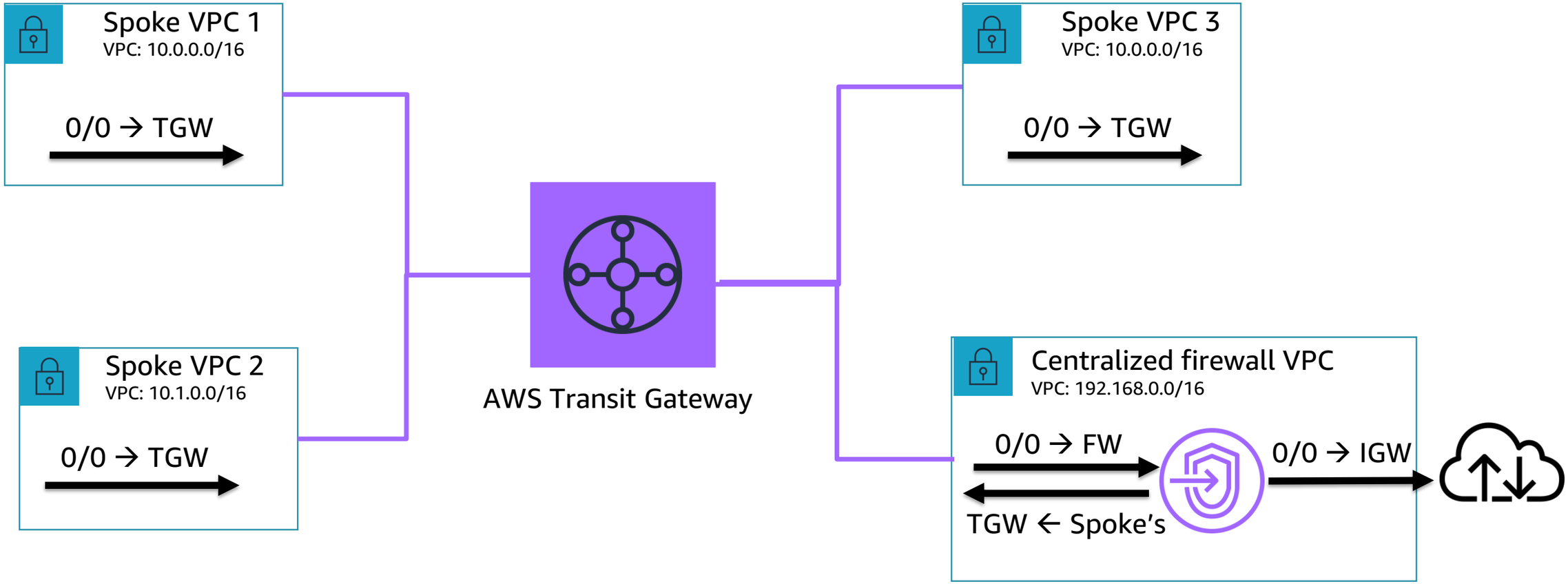
Step 1: 创建防火墙端点



Step 2: 配置VPC路由表



Step2: Network Firewall & AWS Transit Gateway（集中架构）



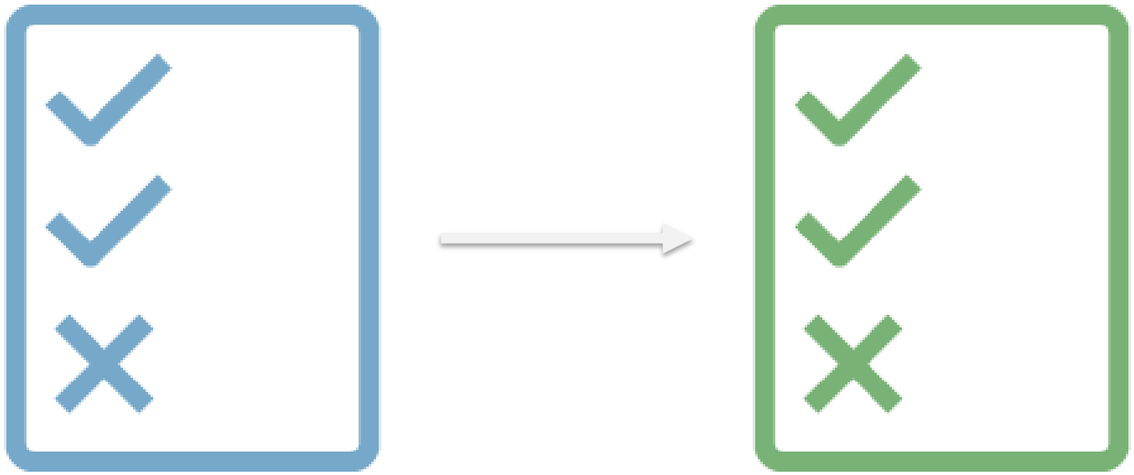
Step 3: 配置策略

每个防火墙都有一个带有多个规则组的策略

规则组可以是无状态的，也可以是有状态的

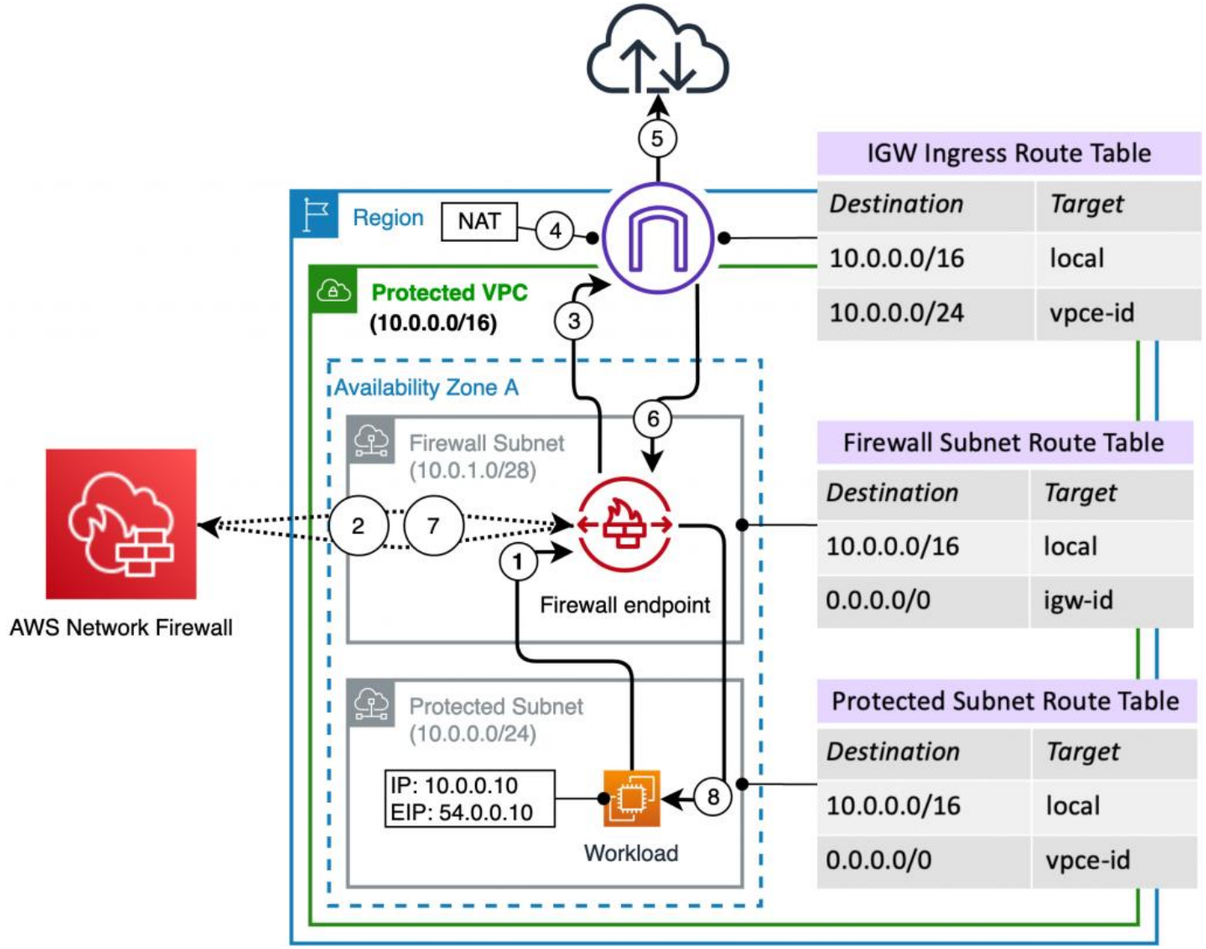
一个策略最多可以包含10个规则组

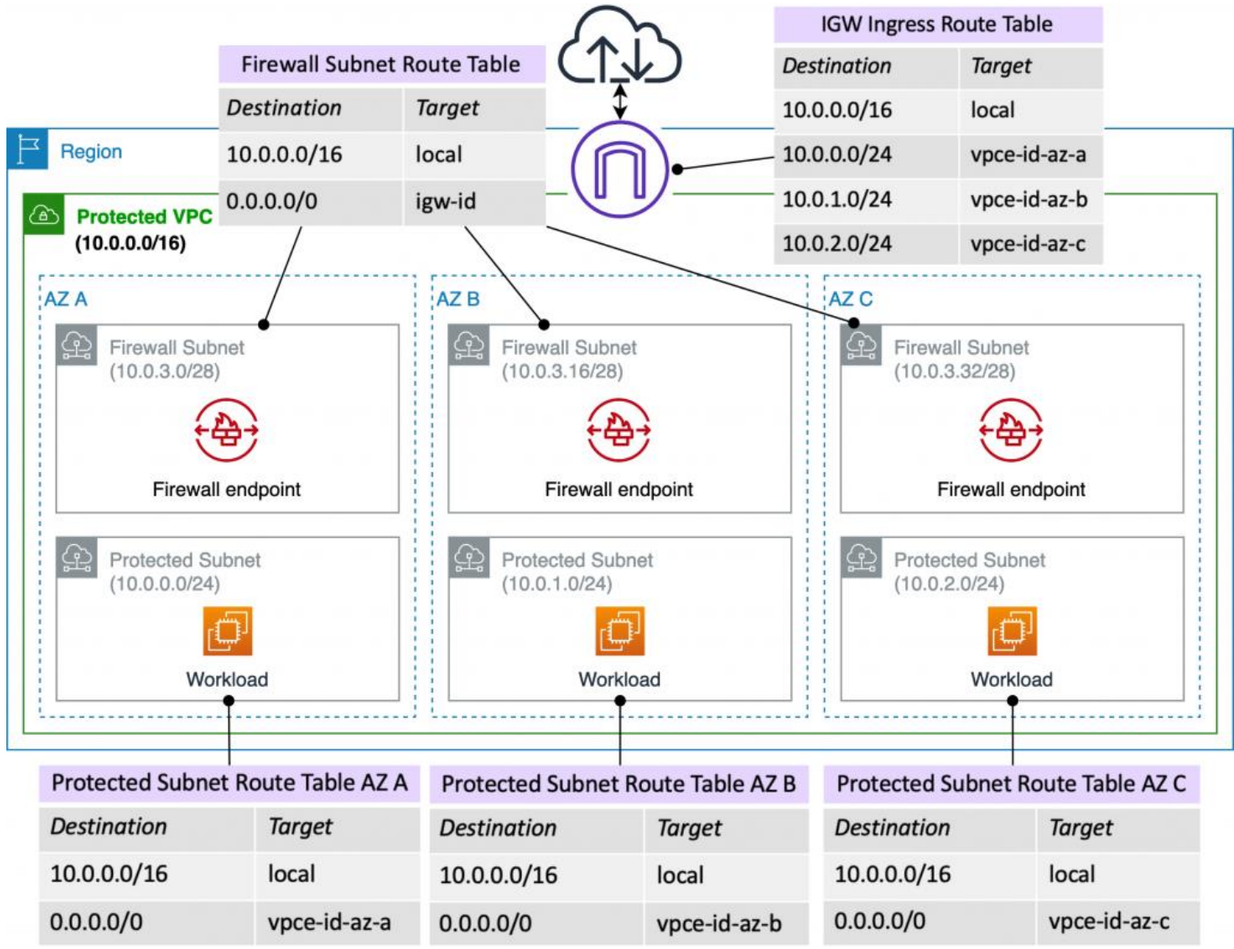
您需要配置一个默认操作



Amazon Network Firewall 参考架构

Single VPC Ingress Protection

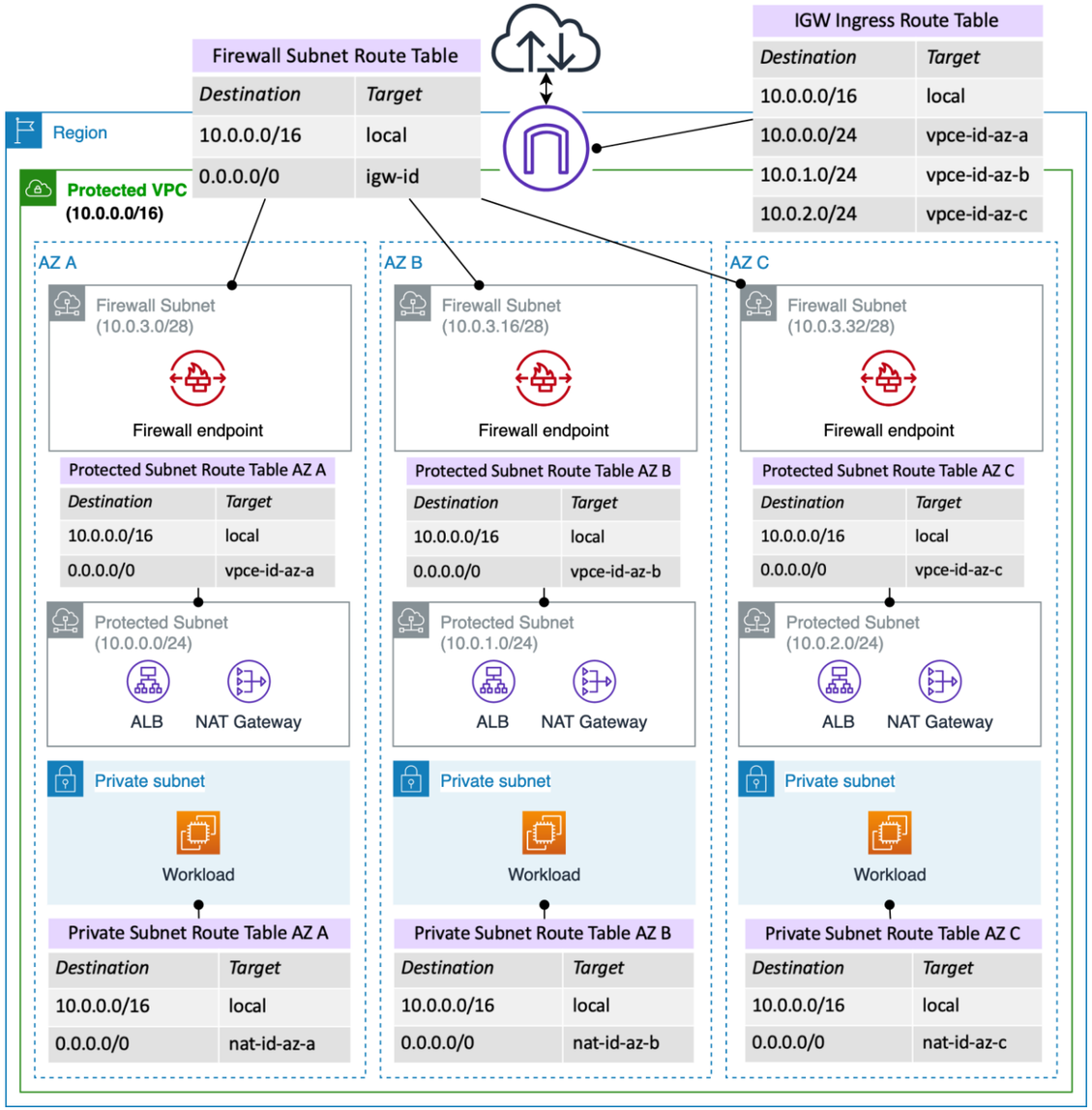




要求：受保护的实例具有Public IP或者EIP

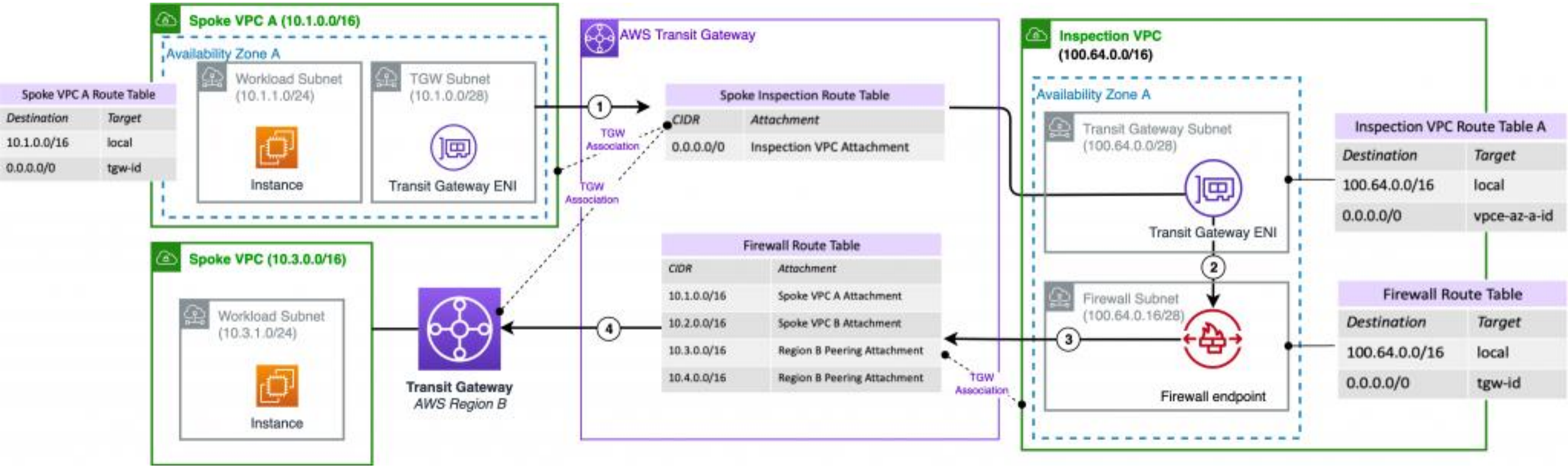
补充：不同AZ内受保护子网的路由表指向本AZ内的Firewall endpoint解决对称路由问题，从而保障有状态流量通过相同Firewall实体进行检测。

Single VPC Ingress and Egress Protection



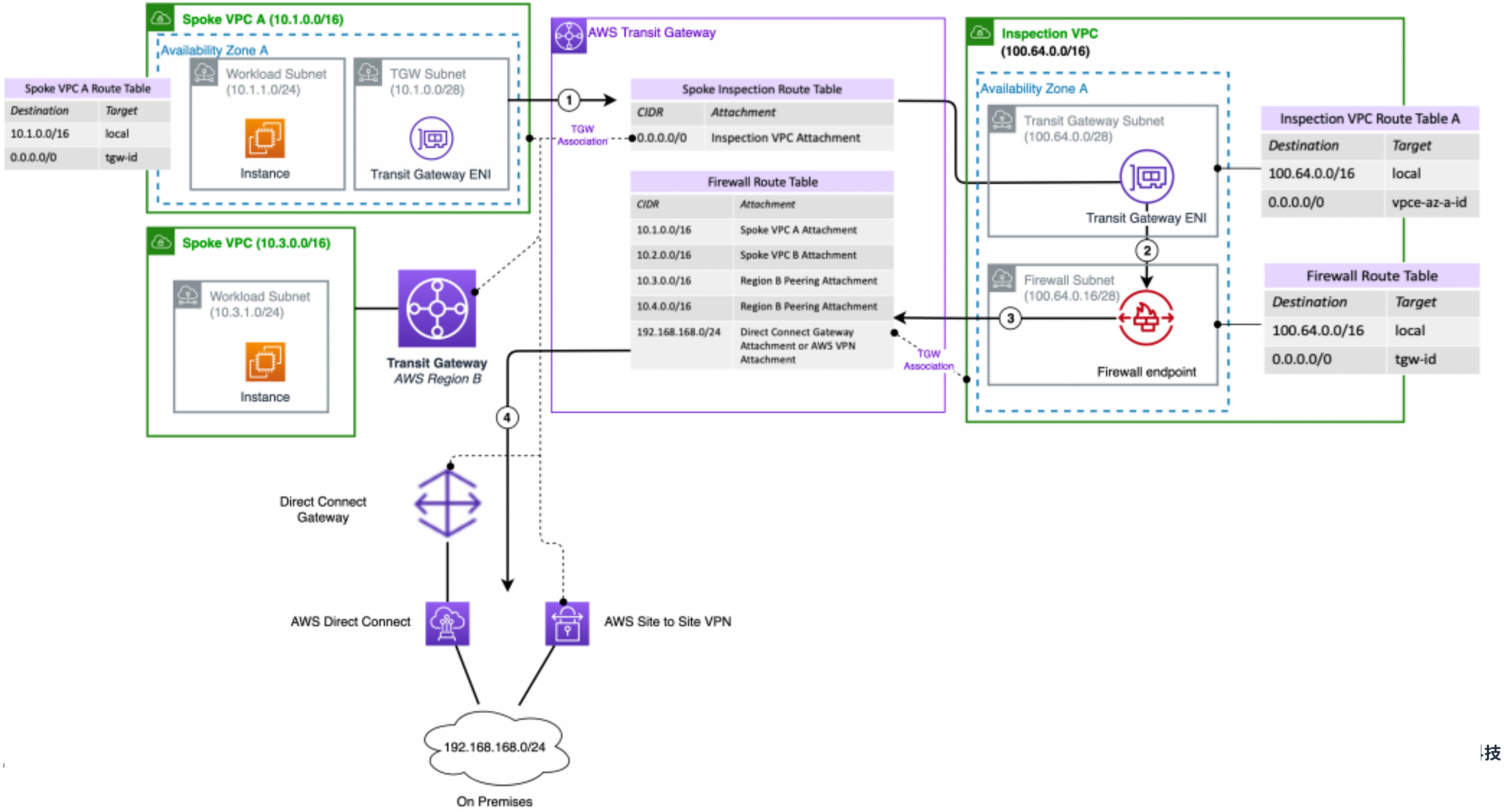
NAT Gateway 必须放置在Network Firewall和受保护子网之间。
目前，不支持其他部署模式。

Multiple VPC without edge protection for East-West Traffic

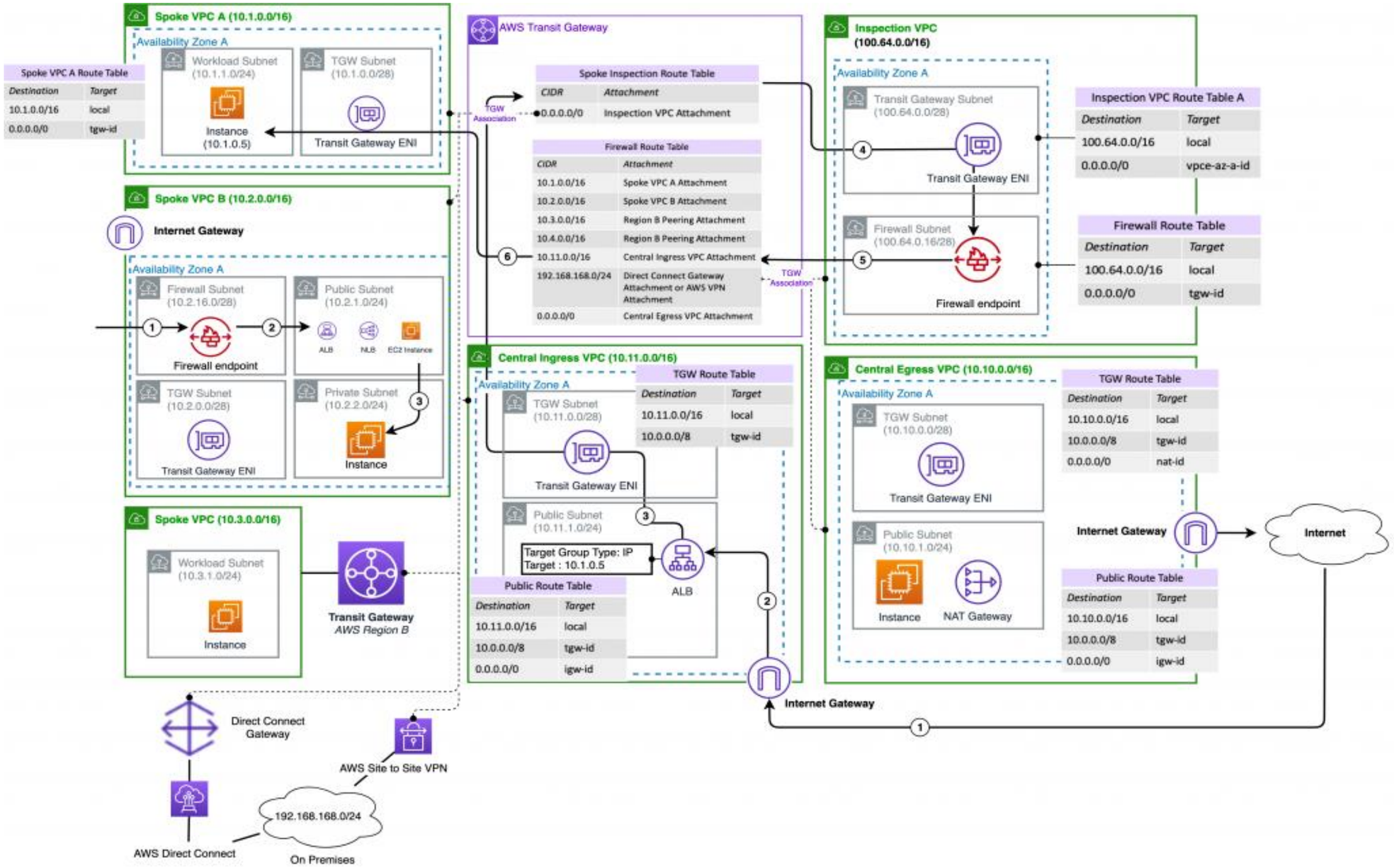


注意Attachment与TGW Route Table 关联关系
如果所有流量均需要通过Network Firewall进行检测，则关闭所有Attachment 的 Propagation。

Centralized on-premises egress & ingress by DX or VPN

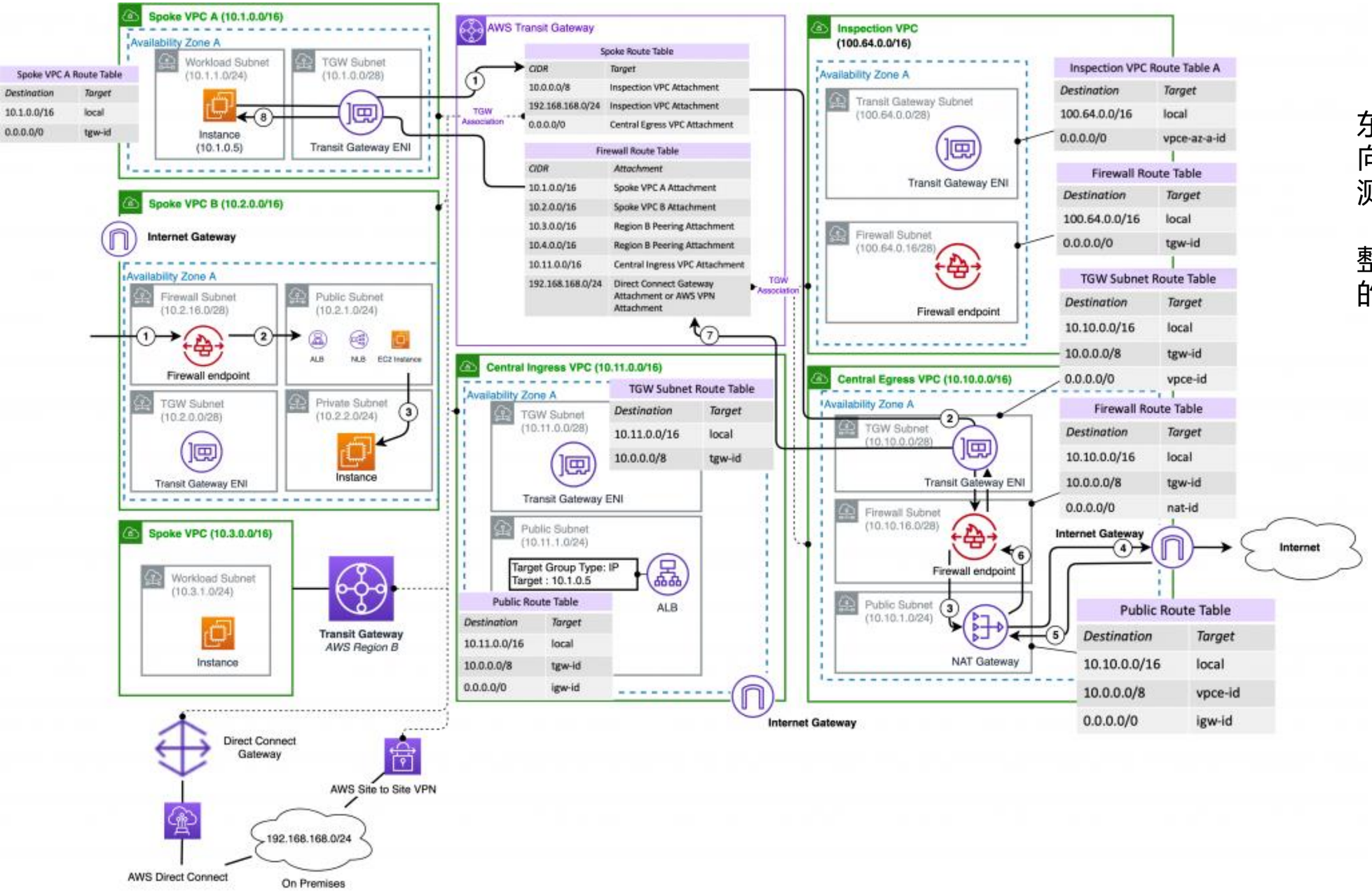


Centralized Internet Ingress via Transit Gateway and NLB/ALB



Ingress 和Egress可分别设立专用VPC，也可以合并为统一的VPC

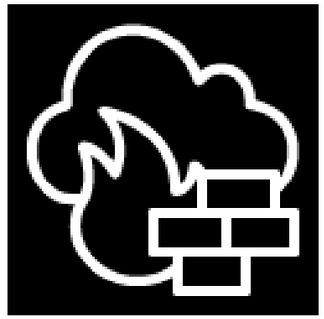
Inspection VPC only for East-West traffic and egress VPC



东西向流量以及整个环境的入向流量均通过专用VPC进行检测

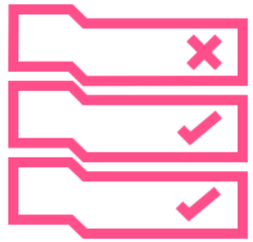
整个环境的出向流量通过独立的出口VPC进行检测

收益



托管

部署灵活



细粒度控制

第三方生态集成

回顾

高可用性，可扩展的防火墙服务

灵活的部署选项

可定制的规则，实现网络分隔和事件日志及入侵检测和防护

与您现有的安全生态系统集成（14家第三方）

不需要预付费用，只需要为你使用的东西付费