РЕФЕРЕНТНА АРХИТЕКТУРА ЗА ПУБЛИЧЕН ОБЛАК IAAS

В Azure имаме Transit Security Services Hub, който е фокусиран върху предоставянето на услуги за сигурност като централна точка на свързаност за всички разширения за влизане, излизане, изток-запад и центрове за данни, мултиоблачно пиъринг и потребителски трафик. Това позволява силно мащабируем и устойчив дизайн за големи организации. Например, инсиращият трафик трябва да има специализирани клъстери за автоматично мащабиране, за да позволи динамични възможности поради променливата пропускателна способност (подобни сценарии, които могат да бъдат намерени в изхода или изток-запад). В случая с разширението на центъра за данни можем да разположим клъстери с висока достъпност за S2S VPN.

Организациите могат да изберат най-добрата си стратегия според своя анализ и да класифицират потоците според следните сценарии:

- Разпръснати приложения.
- Променлива пропускателна способност.

Освен това в AWS имаме транзитен шлюз, който осигурява споделен ресурс за разпределяне на маршрутизиращите домейни за разпределяне на трафика между различни VPC. Домейнът на маршрута е концептуална група от VPC и / или VPN, прикрепени към една маршрутна таблица. От гледна точка на сигурността, този инструмент осигурява гъвкавост за разпределяне на трафика между входящи, изходящи, центрове за данни, мултиоблак и потоци от потребителски трафик. AWS осигурява изключително гъвкава възможност за активиране на нови мрежови архитектури в облака и замяна на много пиъринг връзки от точка до точка.

Макросегменти и микросегменти с транзитни центрове за сигурност

В тази референтна архитектура, която следва принципите hub-and-speak, има пет макросегмента (хъбове за сигурност), където транспортните потоци трябва да бъдат защитени според съответното им поведение.

Макросегменти

- **Frontend Security Hub:** Трафик, свързан с продуктивни системи и обществени услуги (проникване) и трафик, свързан с осигуряване на сигурен достъп до интернет (изход) за различни спици и за целите на поддръжката (изтегляне на кръпки, сервизни пакети и др.).

- **Център за данни или Multicloud Traffic Security Hub:** Трафик, свързан с backhaul комуникации с центъра за данни и multicloud.

- **Отдалечени клонове или MPLS Security Hub:** Трафик, свързан с потребители и отдалечени клонове за достъп до вътрешни производствени системи и корпоративни услуги.
- **Cloud Security Management and Operations Security Hub:** Трафик, свързан с ежедневните операции в облака.
- **Микросегменти**
- **Център за сигурност Изток-Запад:** Трафик, свързан с комуникацията между различните спици.

Следващата таблица показва различната терминология, използвана от доставчиците на облачни услуги.

Таблица 9. Еквивалентни условия между доставчика на облачни услуги

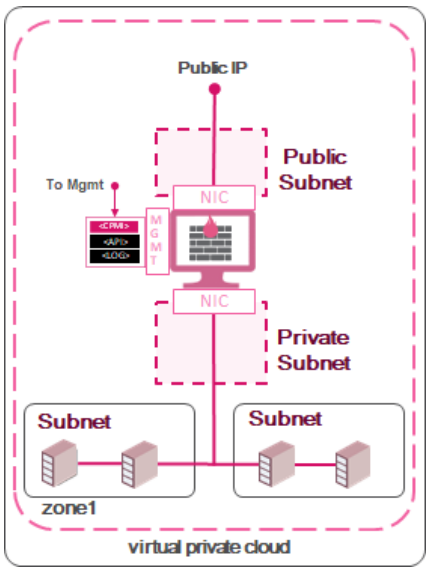
Черта	aws	Microsoft Azure	Google Cloud Platform
География	География	География	География
Зона за наличност	Зона за наличност	Зона за наличност	Зона за наличност
Мрежа	ВПК	ВНЕТ	VPC-Cloud виртуална мрежа
Подмрежа	Подмрежа	Подмрежа	Подмрежа Мрежа
Управление на ресурсите	В конкретна сметка	В целия конкретен абонамент	Глобални, регионални и специфични за зоната ресурси
Виртуална машина (VM)	Екземпляр	Виртуална машина	Екземпляр на виртуална машина
Формат на типа изображение	АМИ	VM изображения	Публично / Частно / Персонализирано изображение
Публични IP адреси	Публичен / еластичен IP	Основен / стандартен IP	Ефимерен / статичен външен IP
Балансиране на натоварването	Приложение / Мрежа / Класически балансьор на натоварването / ELB	Azure Load Balancer, Application Gateway	Външна мрежа и HTTP Балансиране на натоварването, вътрешно балансиране на натоварването
Местни групи за сигурност / сигурност	Групи за сигурност / NACL	Група за мрежова сигурност (NSG)	Правила на защитната стена на компютърната машина
Мащабируеми компютърни инстанции (сървъри)	Еластичен компютърен облак (EC2)	Azure VM	Компютърна машина

Система за имена на домейни (DNS)	Път 53	Azure DNS или Traffic Manager	Облачен DNS
Превод на мрежови адреси (NAT)	NAT шлюзове	NAT шлюзове	Облак NAT
Мрежово пиъринг	VPC пиъринг връзки	Виртуален мрежов пиъринг	VPC мрежа пиъринг
Мрежови маршрути / маршрутизиране	Маршрутни таблици	Azure Virtual Network Routing	Маршрути
Регион	Регион	Регион	Регион
Виртуален частен облак (VPC)	Виртуален частен облак (VPC)	Виртуална мрежа (VNET)	Виртуален частен облак (VPC)
VPC крайни точки	VPC крайни точки	Крайна точка на виртуална мрежова услуга	Частни услуги, частен достъп до Google и/или споделени ВПК
VPN шлюз	Виртуален частен шлюз	Azure VPN Gateway	Облачна VPN услуга
Съхранение на обекти	Кофи S3	Блоб съхранение	Съхранение в облака
Управление на идентичността и достъпа (IAM)	Управление на достъпа до самоличност (IAM)	Azure Role-Based ACL (RBAC) или Azure AD	Облак IAM
Мрежа за доставка на съдържание (CDN)	Облачен фронт	Azure CDN	Свързване на CDN или CDN в облака
Автоматично мащабиране	Група за автоматично мащабиране	Набори от мащаби на VM	Компютърен двигател Autoscaler
Крайни точки на API	API шлюз	Управление на API	Крайни точки в облака

Шлюзове за защита – режими на разполагане

Единичен VPC/vNET шлюз

Това е най-основното внедряване, използвано за осигуряване на разширена сигурност **за малки и средни** работни натоварвания. Този сценарий не предоставя възможности за висока достъпност или мащабируемост. Тя следва да се разглежда само за среди, в които устойчивостта не е основен проблем, и за целите на изпитването.

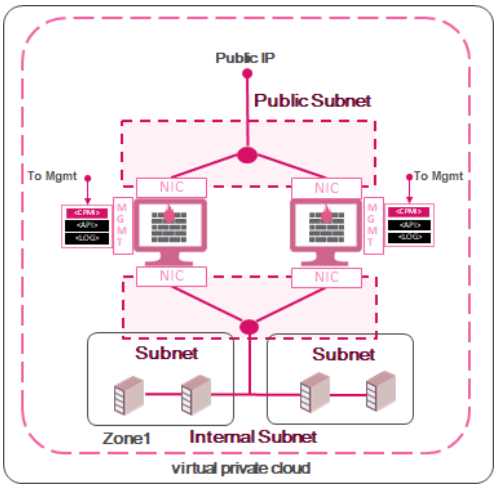


Cloud Service Provider	Supported Scenario
Azure	**Yes, sk109360**
Amazon Web Services	**Yes, sk120534**
Google Cloud Platform	**Yes, sk114577**
Oracle Cloud Infrastructure	**Yes,**
Huawei	**Yes**

Фигура 9. Единичен VPC с единен шлюз за сигурност

Клъстер с висока достъпност единичен VPC / vNET

Клъстерът с висока достъпност е група от виртуални машини, които работят заедно, където един член на клъстера е активен, а вторият член на клъстера е в режим на готовност. Отказът на клъстера от активен член на клъстера до член на клъстера в режим на готовност, когато е необходимо. Този сценарий осигурява усъвършенствана сигурност за трафика изток-запад, когато регулаторните изисквания (NIST, ISO, PCI) изискват видимост и прилагане. Освен това, това е отличен сценарий за обработка на VPN трафик между облаци или backhaul комуникации към локални центрове за данни, особено за високо взискателен трафик като реплики на бази данни.

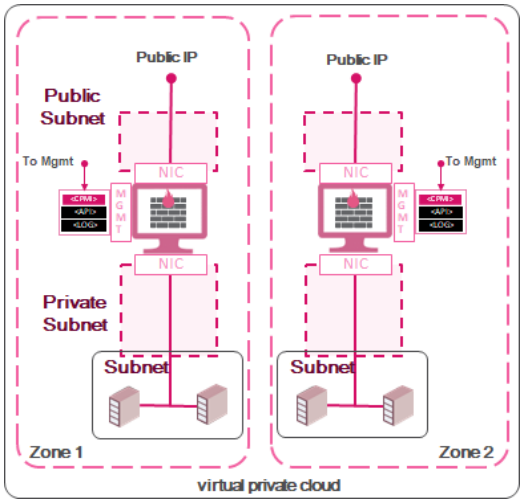


Cloud Service Provider	Supported Scenario
Azure	**Yes, sk109360**
Amazon Web Services	**Yes, sk120534**
Google Cloud Platform	**Yes, sk114577**
Oracle Cloud Infrastructure	**Yes, sk168202**
Huawei	**No**

Фигура 10. Клъстер с висока достъпност, разположен в 1 Z

Два шлюза в две зони на наличност, един VPC / vNET

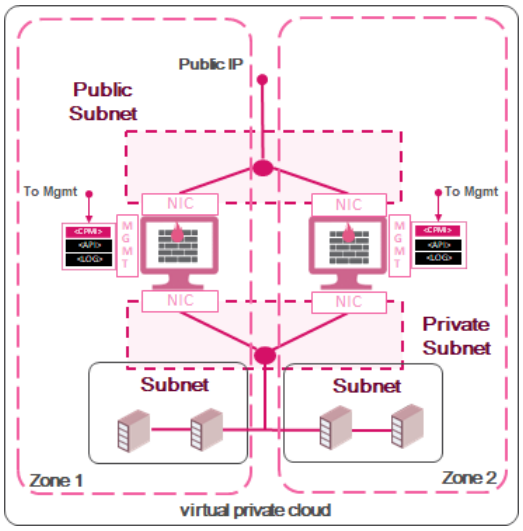
Зоната за наличност е предложение с висока достъпност, което защитава вашите приложения и данни от повреди в центровете за данни. Зоните за достъпност са уникални физически местоположения в рамките на регионите на доставчика на облачни услуги, като всяка зона се състои от един или повече центрове за данни, оборудвани с независими системи за захранване, охлаждане и мрежи. За да се осигури отлична устойчивост, типичният дизайн разглежда минимум три отделни зони. Разгърнатите изчислителни инстанции и шлюзовете за сигурност в различни услуги за излишни зони позволяват възпроизвеждането на приложения и данни в зоните на наличност, предпазвайки от SPOF (единични точки на отказ).



Cloud Service Provider	Supported Scenario
Azure	**Yes, sk109360**
Amazon Web Services	**Yes, sk120534**
Google Cloud Platform	**Yes, sk114577**
Oracle Cloud Infrastructure	**Yes, sk168202**[9]
Huawei	**Yes**

Фигура 11. Архитектура с висока достъпност, като се имат предвид 2 различни зони

Автомащабиране в единична VPC / vNET



Cloud Service Provider	Supported Scenario
Azure	**Yes, sk109360**
Amazon Web Services	**Yes, sk120534**
Google Cloud Platform	**Yes, sk114577**
Oracle Cloud Infrastructure	**No**
Huawei	**No**

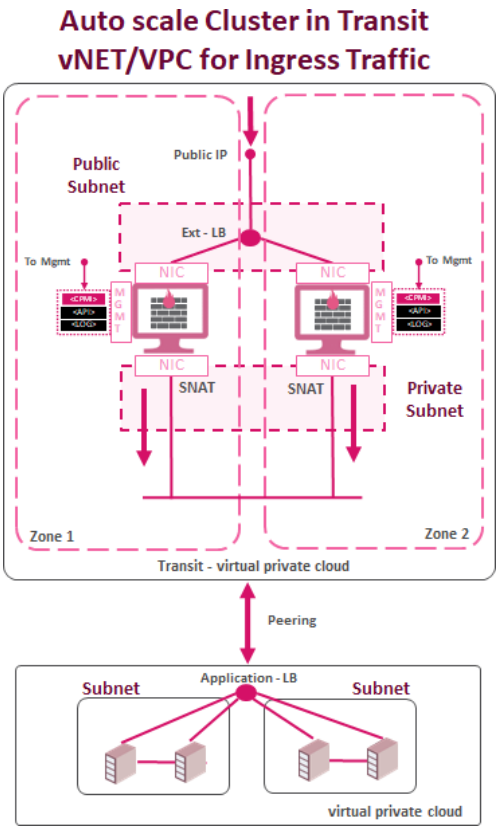
Фигура 12. Клъстер за автоматично мащабиране с шлюзове за сигурност, разпределени в различни зони на наличност.

Autoscale е групиране на изчислителни ресурси, които можете да използвате за разполагане и управление на набори от идентични виртуални машини (VM). Мащабните комплекти увеличават или намаляват броя на виртуалните машини въз основа на текущите нужди. Този тип внедряване е идеално подходящ за работни натоварвания с променлива пропускателна способност, например обществени услуги.

Автоматично мащабиране с транзитен vNET или споделен VPC за входящ трафик

Този сценарий е фокусиран върху инспектирането на входящия трафик чрез транзитна или споделена услуга VPC / vNET с възможности за автоматично мащабиране и променлива пропускателна способност. Типичен сценарий е да се разположи външен балансьор на натоварването за интернет връзки, да се обработва трафикът през шлюза за сигурност и да се постави SNAT, за да се запази симетричен трафикът, след което маршрутизирането може да препрати трафика към съответните VPC / vNET през пиъринга.

Важно е да се отбележи, че в Amazon Web Services имаме Transit Gateway, който е отговорен за препращането на целия трафик към производствения VPC, след като входящият VPC обработва трафика чрез TGW прикачени файлове.

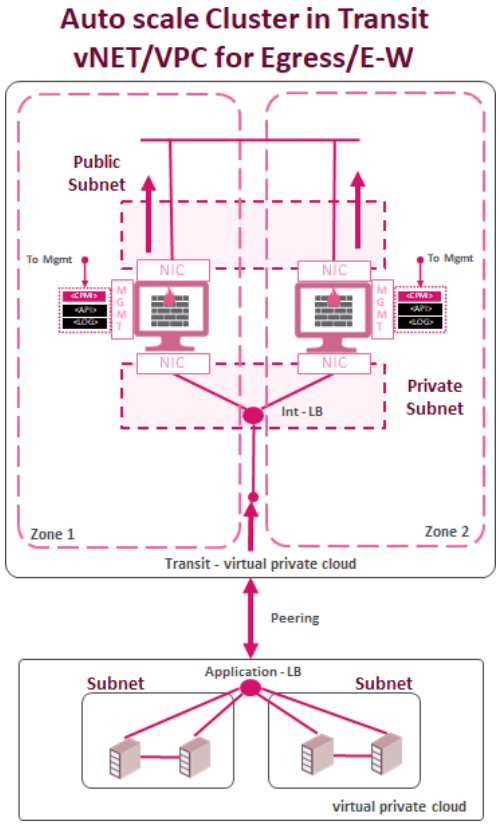


Cloud Service Provider	Supported Scenario
Azure	**Yes, sk109360[10]**
Amazon Web Services	**Yes, sk120534 (through TGW[11])**
Google Cloud Platform	**Yes, sk114577[12]**
Oracle Cloud Infrastructure	**No**
Huawei	**No**

Фигура 13. Autoscale клъстер за проникване трафик с помощта на транзит или споделени услуги VPC / vNET.

Автомащабиране с транзит vNET или споделен VPC за изход и трафик изток-запад

Този сценарий инспектира изходящия трафик чрез транзитна или споделена услуга VPC / vNET с възможности за автоматично мащабиране и променлива пропускателна способност. Типичен сценарий е да се разположи вътрешният балансьор на натоварването за интернет връзки, да се обработи трафикът чрез шлюз за сигурност и да се постави SNAT за публичен IP адрес. Освен това е възможно да се инспектира трафикът изток-запад между различни vNET или VPC. Този сценарий следва да се използва за малки или средни среди, където изходящият трафик не може да споделя портала с изток-запад.

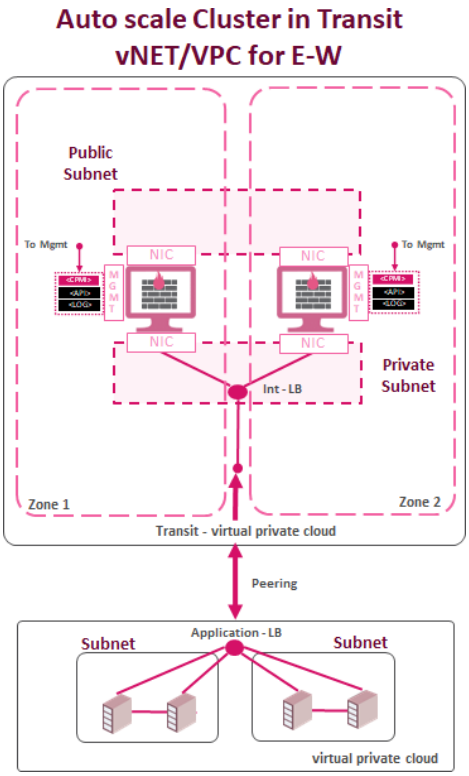


Cloud Service Provider	Supported Scenario
Azure	**Yes**
Amazon Web Services	**Yes, sk120534[13]. TGW[14] VPN with ECMP**
Google Cloud Platform	**Yes**
Oracle Cloud Infrastructure	**No**
Huawei	**No**

Фигура 14. Autoscale клъстер за проникване на трафик с помощта на транзитни или споделени услуги VPC / vNET

Autoscale с транзит vNET или споделен VPC за трафик изток-запад САМО

Този сценарий се фокусира върху инспектирането на различни vNET или VPC (трафик изток-запад), като същевременно осигурява възможности за автоматично мащабиране и обработка на променлива пропускателна способност. Вътрешният балансатор на натоварването е разположен за обработка на трафика между vNET без директна връзка с интернет (този сценарий се отнася за Azure). Въпреки това, в AWS можем да използваме конфигурацията Geo-Cluster или TGW Appliance Mode15, за да осигурим разширени възможности. От друга страна, Google предоставя изток-запад за проверка на трафика между VPC или вътрешни подмрежи.



Cloud Service Provider	Supported Scenario
Azure	**Yes**[17]
Amazon Web Services	**Yes, sk120534**[18] **Also, please refer to the Appliance VPC with TGW Appliance Mode**
Google Cloud Platform	**Yes, sk114577**[19]
Oracle Cloud Infrastructure	**No**
Huawei	**No**

Фигура 15. Клъстер за автоматично мащабиране с шлюзове за сигурност, разпределени в различни зони на наличност.