АРХИТЕКТУРИ ЗА ОБЛАЧНА КИБЕРСИГУРНОСТ, ИЗПОЛЗВАЩИ CLOUDGUARD МРЕЖОВА СИГУРНОСТ

ВЪВЕДЕНИЕ

Разгеждат се случаите на използване, архитектурните диаграми и подхода Zero Trust, който позволява на организациите да изградят по-добра стратегия за сигурност на публичен център за данни в облака.

CloudGuard Network Security ще бъде използвана за проектиране на стратегията, според бизнес нуждите на организацията, в рамките на различни доставчици на облачни услуги.

Желанието за преход от хардуерно ориентирана към ориентирана към приложението мрежова конструкция кара все повече организации да приемат облака като част от своята ИТ стратегия. В резултат на това фирмите бързо приемат решения, базирани на облак, за да виртуализират своите центрове за данни, както и да разширят приложенията и данните в публичната облачна среда.

Тази бяла книга има за цел да предостави на читателя референтни архитектури, използващи различни технически примери, взети от Microsoft Azure, Amazon Web Services, Google Cloud Platform и Check Point Software Technologies, както и от различни технически блогове. Информацията, представена в тази статия, има за цел да образова и даде възможност на инженери по сигурността и мрежите, архитекти на решения и дизайнери, които биха искали да интегрират публични облачни IaaS решения и технология Check Point за напреднала сигурност. За да извлече максимума от тази статия, читателят трябва да бъде добре запознат с облачните изчисления, дизайна на мрежата и сигурността, както и с методологиите на Zero Trust.

Според Gartner Forecasts for Worldwide Security and Risk Management Spending, през 2020 г. инвестициите в облачна сигурност са нараснали с 33,3% спрямо 2019 г. Тъй като все повече организации са убедени, че трансформацията на облака ще доведе до по-големи бизнес възможности и оперативна гъвкавост, те трябва да осъзнаят последиците за киберсигурността в процеса. Трансформацията не трябва да се разглежда като промяна 1 към 1, която отчита само традиционния подход; по-скоро трябва да бъде съобразена с бизнес стратегията и апетита за риск.

При този подход организациите трябва да разберат три различни миграционни модела, свързани с миграцията в облака, като вземат киберсигурността като основен двигател:

- **Rehost (lift-and-shift)** – Организацията мигрира работните си натоварвания както е, без рефакториране или възстановяване и използвайки един VPC. Контролите за киберсигурност също се мигрират от 1 към 1, като се използват почти същите политики за сигурност. Тази стратегия може да бъде с висок риск поради липсата на подходяща видимост и управление на конфигурацията.

- **Рефакторинг и контейнеризация** – Приложенията на организацията са отделни компоненти, консумиращи различни библиотеки и зависимости за трансформиране на информация за данни. Микросегментацията на приложението има отделни контейнери, свързани с фронтенд, бекенд и споделени услуги, където потоците трафик се разделят между входа, изхода, изток-запад и backhaul. Специфичните проверки за сигурност се вземат предвид за правилното прилагане и видимост.

- **Възстановяване (shift-and-lift)** – Бизнес процесът на организацията се нуждае от пълен редизайн, за да създаде облачни приложения. На този етап платформите за защита на приложенията в облака са от съществено значение за подобряване на политиките за киберсигурност и за осигуряване на по-значително предимство в облака.

Какво е „lift-and-shift“?

Основната цел на lift-and-shift е да се запазят същите архитектурни организации, които вече имат в публичния облак, без да се правят значителни промени в дизайна. С други думи, това е процесът на мигриране на идентично копие на работното натоварване (включително операционната система, приложенията и данните), проектирането и управлението на мрежата, както е. Това го прави най-бързият и най-евтиният път. От гледна точка на сигурността, той също така запазва същите системи за управление и дори запазва същите политики за сигурност, поне в началния етап на трансформацията в облака. Lift-and-shift е най-често срещаният първи етап от общото пътуване за трансформация на облака, тъй като е сравнително лесен и бърз за постигане.

Повдигането и смяната носи няколко предимства за цялостната позиция на сигурността и операциите на организациите, като например:

- Автомащабиране, пъргавина и скорост.
- Разгръщане на динамична инфраструктура, нулево доверие и микросегментиране.
- Адаптивна и динамична сигурност в облака.
- Преход от CAPEX към OPEX.

Въпреки това, организациите трябва да внимават да не объркат модела на миграция с копиране и поставяне. Такова недоразумение може да доведе до катастрофа, ако се мигрират грешки в дизайна, особено в системите за сигурност без правилния контрол и политики, влияещи върху нивото на обслужване.

Оптимизиран модел за повдигане и превключване

Check Point препоръчва нов модел на миграция, който позволява на организациите да имат по-голяма гъвкавост, гъвкавост, скорост, мащабируемост, динамична сигурност и управление на стойката, за по-добър модел на споделена отговорност в своите стратегии за центрове за данни в облака. Този модел, наречен **Lift-and-Shift Optimized**, позволява хармонизиране на принципите на хъб и спици и разширена рамка на Zero Trust2, за да осигури пълна видимост и контрол на сигурността и съответствието. Следователно, той помага да се сведе до минимум повърхността на атаката и предпазва от уязвимости, идентифициране на кражби и загуба на данни. Предложеният от нас модел може да се използва като първа стъпка за мигриране на работни натоварвания, които са кандидати за миграция към облака.

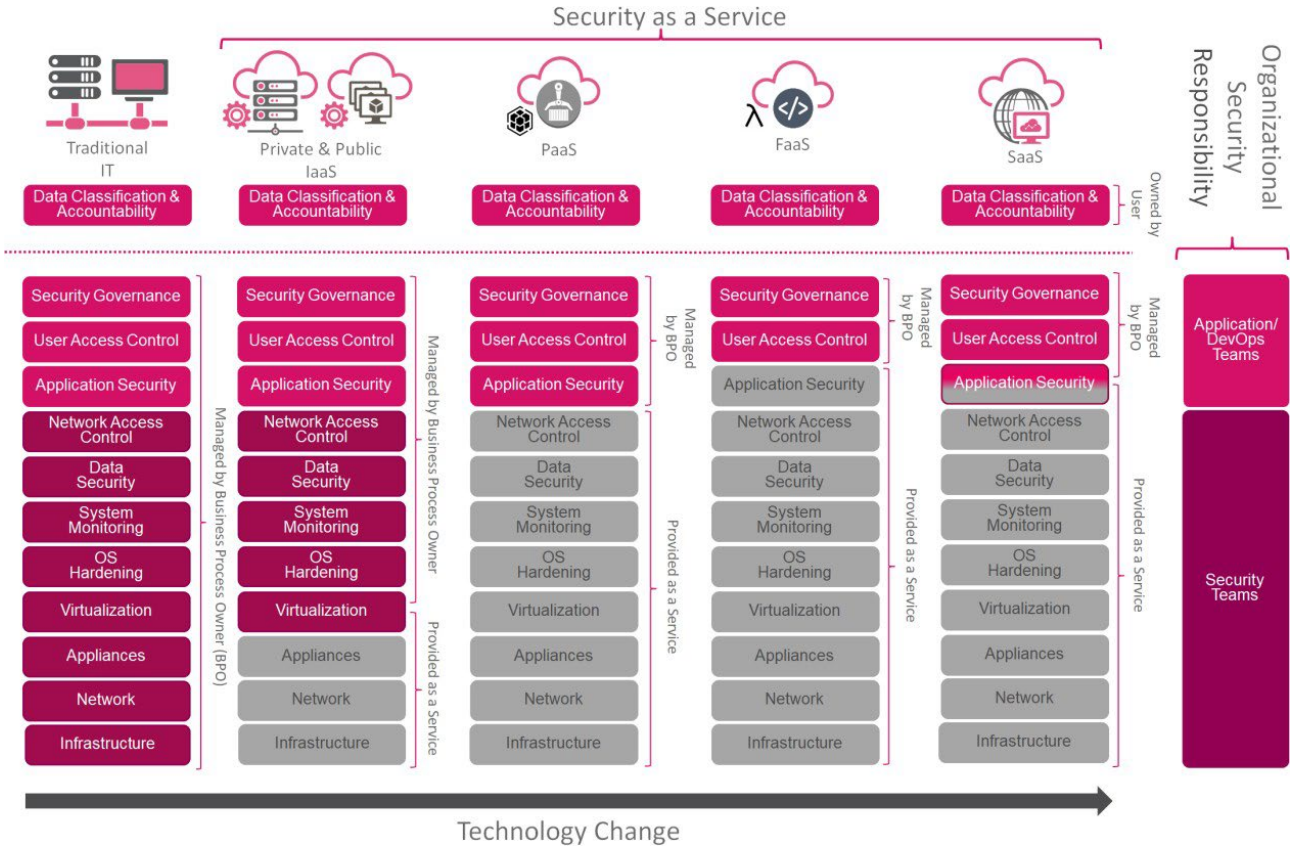
В следващите раздели ще представим различни случаи на употреба с референтни архитектури, където CloudGuard NS (Cloud Network Security, известен още като CloudGuard IaaS) може да осигури стабилно решение за осигуряване на всички комуникационни потоци в VPC на организацията за мулти-облачна стратегия, разполагаща Azure и Amazon Web Services. Освен това ще обясним значението на внедряването на CloudGuard Posture Management като единично стъкло, за да се осигури управление на състоянието на сигурността за внедряване на IaaS в мулти-облачни архитектури, като по този начин се опростят операциите за сигурност в облака.

Споделена отговорност за публичните IaaS

В традиционните ИТ среди организацията притежава целия стек, а специализираният екип по сигурността прави необходимите промени в инфраструктурата. В публичния облак IaaS някои отговорности се прехвърлят на доставчиците на облачни услуги, а някои се прехвърлят на собствениците на приложения.

Доставчиците на облачни услуги са отговорни3 за гарантиране на сигурността на самата облачна среда, но екипите за ИТ сигурност отговарят за контрола на сигурността на инфраструктурата, за която отговарят. След като дадена организация се премести в PaaS / FaaS и SaaS, някои отговорности ще

бъдат прехвърлени на групите DevSecOps. Въпреки това водещата изследователска и консултантска компания Gartner заяви, че "до 2020 г. 99% от провалите в сигурността в облака са по вина на клиента". 4 Това означава, че екипът по мрежова сигурност все още е отговорен за постоянната зрялост на всички конфигурации, свързани с водопровода на облачния център за данни. Следователно инструментите за управление на сигурността на мрежата в облака и облачната сигурност за публични IaaS осигуряват един панел от стъкло за правилното внедряване на контролите на Zero Trust.



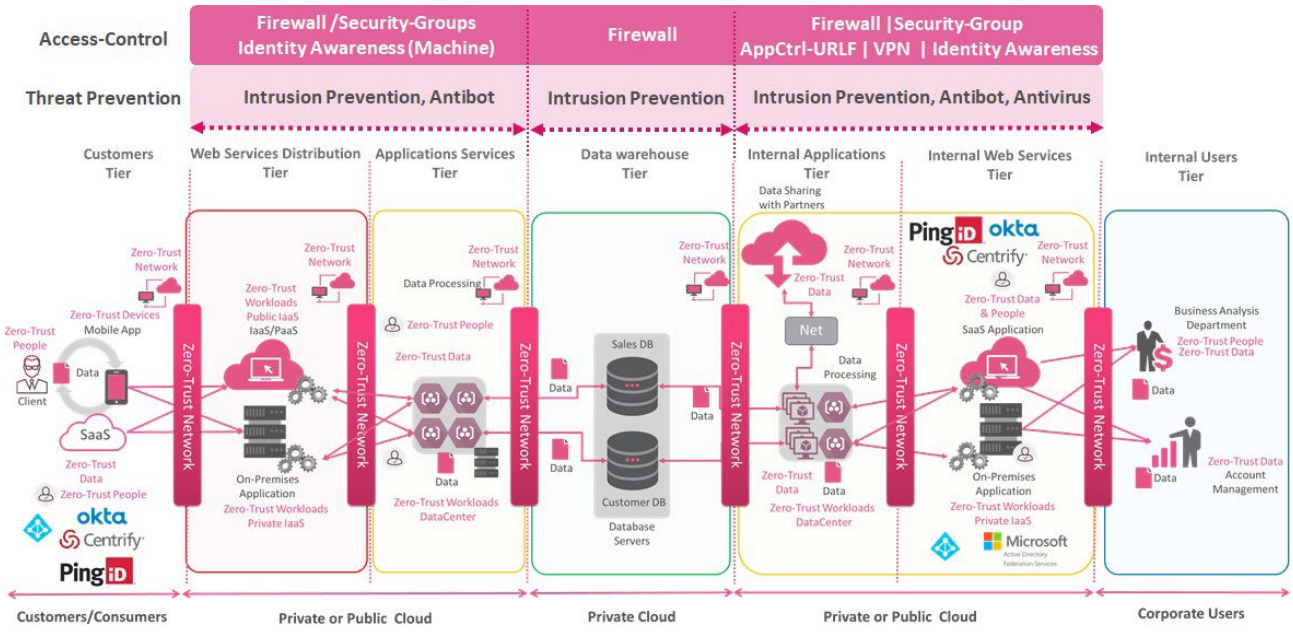
Фигура 1. Разширен модел за споделена отговорност за публични IaaS.

Модел на нулево доверие

Споделената отговорност, съобразена с принципите на Zero Trust, осигурява по-добро хармонизиране на контрола за сигурност, като помага да се сведат до минимум потенциалните рискове в процеса на миграция, особено в ежедневните операции. В този раздел ще обясним как принципите на мрежата и работното натоварване на Zero Trust са по-малко сложни, като се има предвид подходът на хъб и говори и ориентираната към услугите5 архитектура (SOA), използвана за защита на приложенията и услугите на организацията.

Рамката за нулево доверие разглежда следните стълбове:

- **Данните:** Ядрото на бизнеса.
- **The Workloads:** Спици, които трансформират данни в информацията.
- **Мрежите:** Центрове, където данните и информацията се транспортират с помощта на микросегментиране и механизми за криптиране от край до край.
- **Устройствата:** Крайни точки или IoT устройства, които имат достъп до данни в хъбовете.
- **Хората:** Които консумират информация, използвайки приложения, предоставени от спиците. Също така включва администраторите за управление на операциите за сигурност в облака чрез позата за сигурност.



Фигура 2. Референция за архитектура с нулево доверие: Архитектура за публични и частни IaaS.

Правилните политики за сигурност между уеб нивото, ориентираното към услугите ниво на приложение и нивото на базата данни позволяват на организацията да има много по-добра стойка в облачната среда, за да защити различните активи в публичните IaaS, като по този начин минимизира рисковете. Докато SOA е традиционният подход, който организациите следват в процеса на миграция, след като започнат да мигрират към микросервизите, моделът SOA също трябва да бъде трансформиран.

Сегментиране на сигурността на IaaS

IaaS сегментацията има за цел да намали радиуса на взрива и да позволи на екипите за сигурност да наложат контрол за сигурност на периметъра. Два мощни варианта улесняват тези възможности: микросегментиране и макросегментиране. В следващата таблица ще разгледаме разликите между инструментите и техните практически приложения за сегментиране на IaaS.

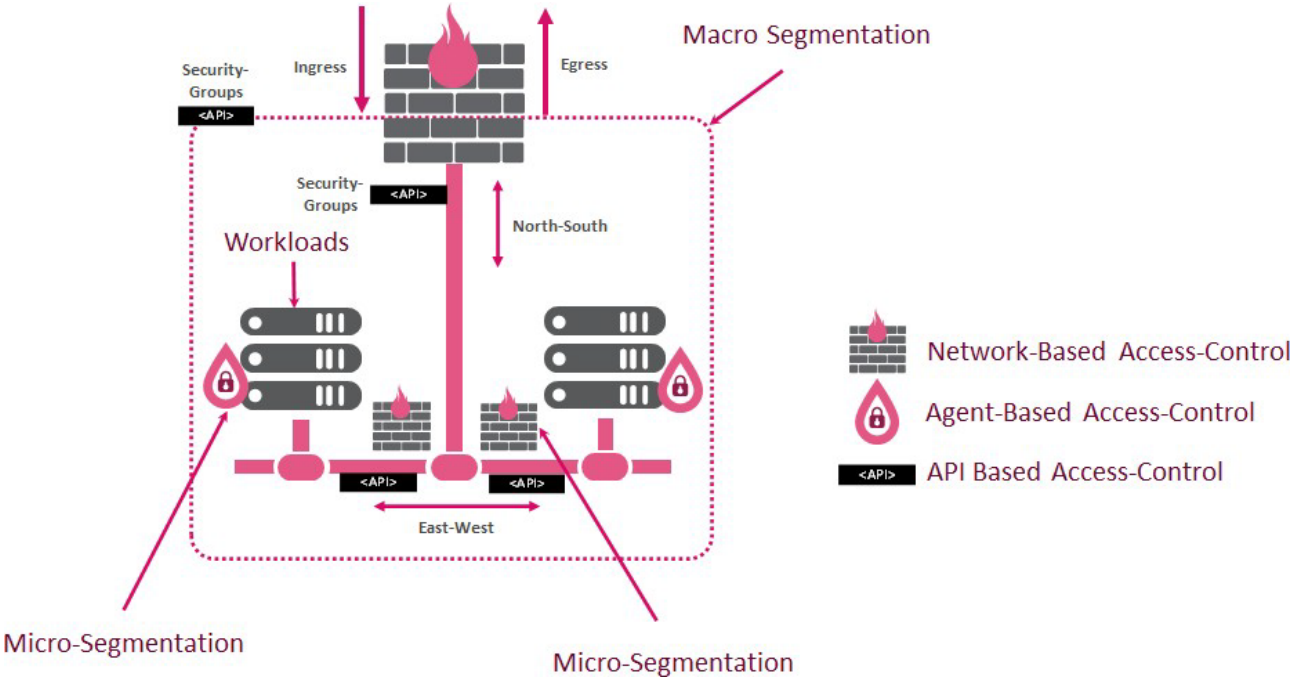
- **Макросегментиране:** Създава зони за защита в цялата мрежа, за да предотврати атаки между основните сегменти на сървъра, като използва множество натоварвания с една и съща функционалност и класификация на защитата.
- **Микросегментиране:** Логично разделя vNET / VPC на отделни сегменти за сигурност до индивидуални нива на натоварване. Такова детайлно ниво, при което микросегментацията контролира трафика на работното натоварване, минимизира заплахите за сигурността и създава модел за сигурност Zero Trust. За публичния облак CPM на Check Point осигурява централизирано управление и може да се прилага за индивидуални натоварвания, което позволява по-сигурна среда без допълнителни режийни разходи за специфична за работното натоварване конфигурация.

Таблица 3. Атрибути на микросегменти и макросегменти.

	Публична IaaS микросегментация	**Публична IaaS макросегментация**
Случай на използване	Използва се за логическо разделяне на VPC / vNET на различни зони за сигурност, до индивидуално ниво на натоварване	Използва се за разделяне между основни групи работни натоварвания с подобна функционалност и класификации за сигурност (като уеб сървъри, сървъри за приложения и бази данни), предотвратявайки движението на нападателите в периметъра и атакувайки производствените натоварвания
Обхват	По-гранулиран, тъй като контролира страничното движение между гостоприемниците	Повече за нивото на периметъра и в зоните за сигурност
Политики	Подробни политики от хост към хост	Политики на ниво мрежа/сегмент
Прилагане на политиката	Изчислителни инстанции	Подмрежа/VLAN
Управление и контрол	Политики за сигурност от хост към хост за контрол на достъпа или предотвратяване на заплахи	Функционални политики за сигурност vNET/VPC за контрол на достъпа или предотвратяване на заплахи

Контрол на комуникацията хост-към-хост	Между работните натоварвания в един и същ сегмент	Ниво мрежа или зона за сигурност
Контрол на траекторията на трафика	Изток-запад или страничен трафик	Север-юг и изток-запад (проверете трафика между уеб, приложение и DB зони)
Ползи	- Налагане на сегментация на ниво гранулирано ниво в рамките на една и съща група приложения. Критичните приложения ще останат безопасни дори в случай на нарушение - Прилагане на правила до слой 7	- Налагане на сигурност в периметъра, за да се предпази от атаки - По-лесен за изпълнение от микросегментацията
Недостатъци	Необходими са умения на високо ниво, включително видимост на ниво приложение, за да се използва микросегментиране	Усъвършенствани умения за мрежа и сигурност за внедряване на политики за сегментиране, базирани на мрежата

Използването на макросегментиране и микросегментиране може да помогне на организациите да направят по-добър избор по отношение на контролите за защита, които могат да се използват според потоците от приложения. В допълнение, контролът на достъпа може да бъде внедрен в три различни сценария: мрежово-базиран, базиран на агент или хост-базиран и API, използвайки инструменти в облака.



Фигура 4. Макросегментиране и микросегментиране

Диаграмата по-горе осигурява визуално представяне на всички потоци, защитени в публичния IaaS. С тази перспектива следващата таблица предлага различни сегменти на защита според потоците, което ви позволява да изберете необходимите контроли по-точно.

Таблица 5. Подравняване на остриетата за сигурност със сегментите за сигурност

Сегмент за защита или концентратор за защита	Потоци	Сигурност
Проникване на трафик от интернет	Контрол на достъпа север-юг и инспекция на трафика	Защитна стена, базирана на правила IPS, SSL инспекция
Изход на трафика към интернет за изчислителни инстанции, Azure Virtual Desktop или Amazon Web Services Workspaces	Контрол на достъпа север-юг и инспекция на трафика	Защитна стена, контрол на приложенията, URLF, Antibot, Antivirus, SSL инспекция или HTTP категоризация
Трафик между различни vNETs/VPC и работни натоварвания	Контрол на достъпа изток-запад	Групи за мрежова защита или защитна стена
Трафик между различни vNET/VPC и натоварвания	Инспекция на движението Изток-Запад	Защитна стена, базирана на правила IPS
Трафик от SD-WAN/MPLS (Backhaul)	Север-юг	Защитна стена, IPS, базирана на правила, осведоменост за идентичността
Трафик между OnPremises център за данни (backhaul)	Север-юг	Защитна стена, базирана на правила IPS
Трафик между доставчици на мулти-облачни услуги (backhaul)	Север-юг	Защитна стена, базирана на правила IPS, VPN

При този подход моделът на споделена отговорност е по-достъпен за ежедневните операции. Transit Security Services vNET (Azure), Transit Gateway (Amazon Web Services) и Shared VPC (Google) осигуряват на облачните центрове за данни по-добра мащабируемост и позволяват мрежовите принципи на Zero Trust, свързани с функционалната сегментация.

Принцип „Hub-And-Spoke“

Този раздел ще разгледа модела hub-and-spoke, препоръчан от Microsoft. Накратко, облачната среда е създадена като система от връзки, в която всички спици са свързани с транзитен хъб, а целият трафик към и от

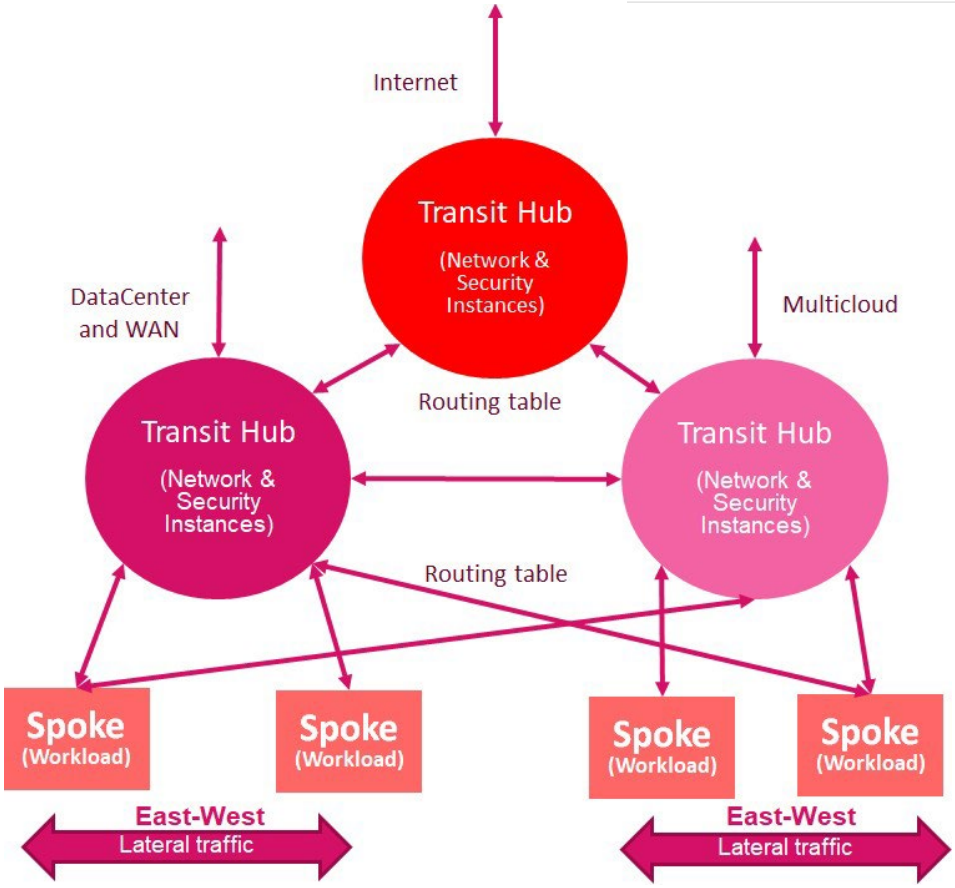
спиците преминава през транзитния център. Основният фокус на този принцип е да осигури по-практична сегментация на стратегиите за повдигане и смяна, когато vNET / VPC се използва за осигуряване на по-лесна настройка за Zero Trust мрежа в облака. Въпреки че можем да сегментираме в рамките на vNET / VPC, няма лесен начин да наложим инспекция на трафика, тъй като доставчиците на облачни услуги контролират цялото маршрутизиране в периметъра на vNET / VPC.

Важни определения

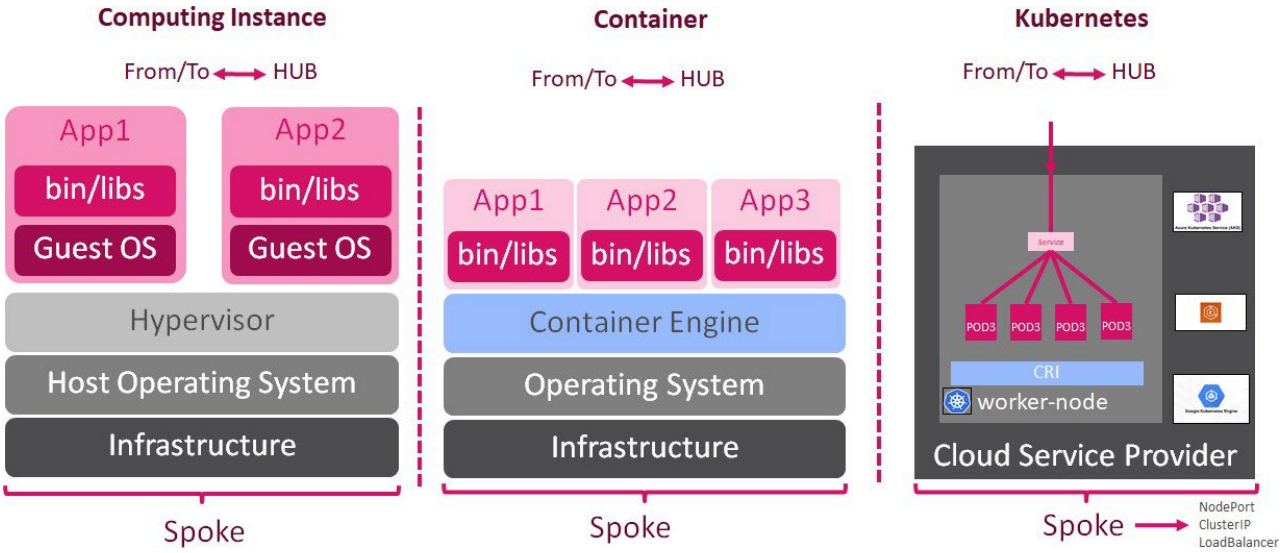
Spoke е изолирана мрежова среда, която съдържа колекция от една или повече мрежови подмрежи, от които могат да се инсталират и изпълняват типични натоварвания. Типичен случай на употреба е спица, която съдържа няколко виртуални сървъра, които съставляват или част от, или цял стек от приложения (уеб, приложение и база данни). Друг случай на използване е спица, която действа като разширение на съществуващите локални мрежи, като например набор от QA сървъри за тестови цели или набор от сървъри за обработка на данни, които използват осигуряването при поискване на облака за по-ниска цена и подобрена гъвкавост.

Въпреки това, от гледна точка на сигурността, имаме различни спици, които могат да бъдат разположени в публичните IaaS: Transit Hubs.

Изчислителни екземпляри, контейнери при поискване или като услуга Kubernetes клъстери, крайни точки на услугата или VPC крайни точки без сървър или сервизни функции



Фигура 6. Hub-and-Spoke архитектурни принципи



Фигура 7. Примери за различни спици за обществеността IaaS

Транзитният център позволява гъвкавост и систематично разделяне на комуникационните потоци през околната среда. Тя може да бъде предназначена за трафик на проникване, страничен трафик между спиците, трафик в / извън корпоративната мрежа или за изходящ трафик към интернет или други облачни среди. Маршрутизиращият трафик може лесно да бъде конфигуриран според транспортните потоци* в приложенията.

*В следващия раздел ще обясним потоците в транзитните центрове и използваните взаимодействия, за да изградим правилния водопровод за инфраструктурата

Transit Security Hub е Azure Transit vNET или Amazon **Web Services Transit Gateway** и GCP **Shared VPC**, който свързва всички виртуални облачни и локални мрежи. Концепцията за транзитна сигурност се определя като точка за контрол на сигурността за междусистемните връзки в облачните мрежи и междуспициозната сигурност. Хъбовете са единственият начин за влизане / излизане от околната среда, както и единственият начин за преминаване вътре и между спиците в околната среда. Това се дължи на това, че спиците не са свързани директно, а са достъпни само чрез един от центровете. Ключов елемент е маршрутизирането и конфигурацията на връзката между хъбовете и спиците (UDR, статично маршрутизиране или BGP за по-сложни среди).

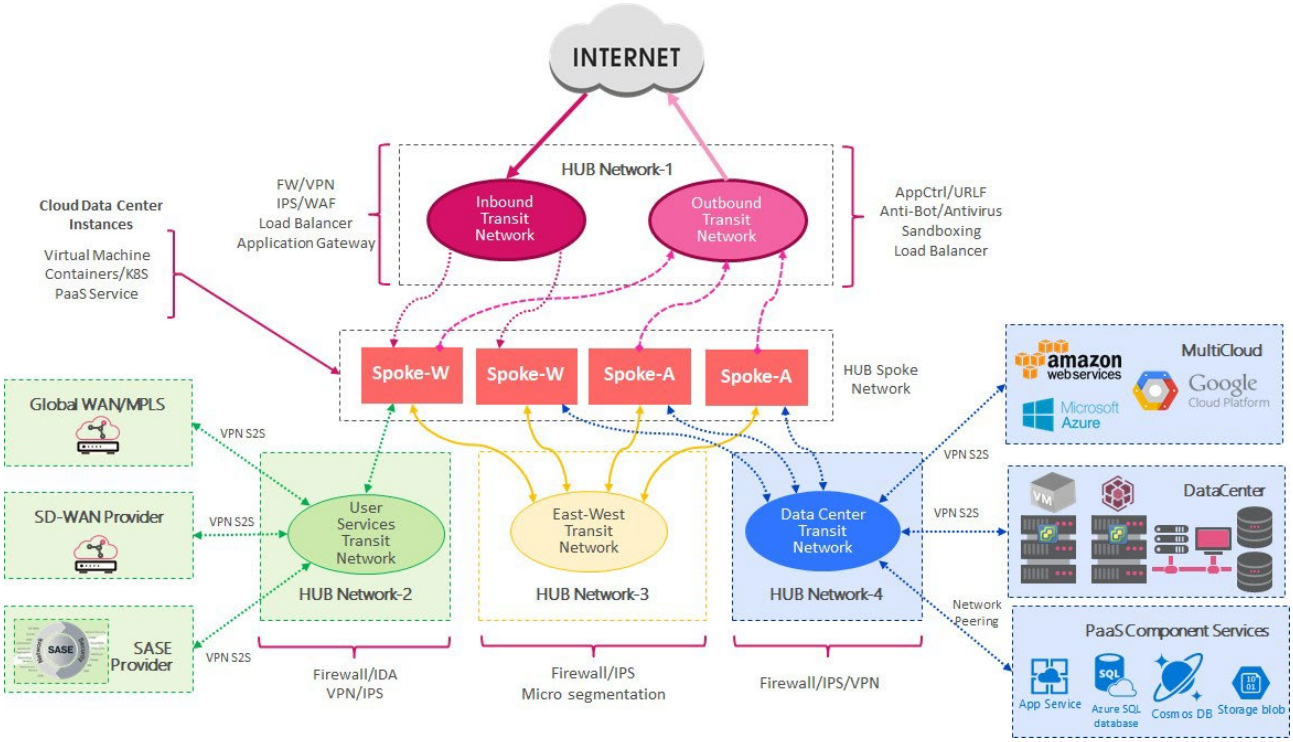
Дизайн за сигурност на високо ниво

Дизайнът за мрежова сигурност на хъб и спици осигурява централен компонент, свързан към множество мрежи около него, което позволява различни контроли за сигурност. Настройването на тази топология в традиционния локален център за данни може да бъде скъпо, но в облака няма допълнителни разходи. Оптимизираният модел за повдигане и превключване позволява да се изградят мощни сценарии за мрежи и сигурност в публичните IaaS, които от своя страна дават възможност на организациите да имат различни сценарии, осигуряващи агностичен подход:

- Създаване на отделни среди за разработка и производство с активирани различни контроли за сигурност.
- Изолиране на работните натоварвания на различни клиенти, използвайки възможности за микросегментиране и предотвратяване на заплахи.
- Сегрегиращи среди, за да отговарят на изискванията за съответствие, например PCI, GDPR и HIPAA.
- Сегрегиране на среди с помощта на контроли за сигурност в облака, които използват инструменти за управление на позата на сигурността в облака.
- Предоставяне на споделени ИТ услуги, като active directory, DNS и

файлови сървъри.

- Multicloud сигурност като код с автоматизация в осигуряването на инфраструктурата за сигурност на облака като код, използвайки CI / CD тръбопроводи с Terraform, Jenkins, Puppet и Ansible.



Фигура 8. Транзитни хъбове и спици: оптимизиран модел за повдигане и превключване.

В оптимизирания модел за повдигане и превключване имаме четири различни типа хъбове с различни функции за сигурност:

А. Интерфейсен хъб

Фокусиран върху осигуряването на комуникации към обществените мрежи с два вида трафик: проникване и излизане.

- Перспективата за проникване изисква само контрол на достъпа като защитната стена и IPS с механизъм за проверка на SSL или уеб приложение и API защита.
- Изходната перспектива изисква контрол на достъпа за приложения и уебсайтове. Общият сценарий е да се осигури сигурен достъп до интернет на работните натоварвания за изтегляне на поправки, кръпки, библиотеки и др.

Б. Център за разширение на център за данни

Фокусиран върху предоставянето на комуникации от локални центрове за данни и мултиоблачни комуникации.

- Контрол на достъпа като защитна стена / VPN и предотвратяване на заплахи, интегриране на IPS и антивирус за проверка на трафика от локално до центъра за данни в облака.

В. Център Изток-Запад

Фокусиран върху целия страничен трафик между различните спици.

- Микросегментиране за контрол на достъпа: използване на инструментите за контрол на достъпа в облака, за да се осигурят основни възможности за защитна стена, за да се разрешат или откажат конкретни услуги.
- Микросегментиране за предотвратяване на заплахи: използване на усъвършенствани възможности за инспекция на трафика, осигуряващи виртуално управление на кръпката.

Г. Център за потребители или споделени услуги

Фокусиран върху свързването на потребителите от отдалечени клонове с ресурсите, разположени в центъра за данни в облака.