Kutatói munka leírása

Virtuális vagy fizikai tűzfal választásának kritériumai, NISZ Zrt.

Szerző: Leiter Ákos (Budapesti Műszaki és Gazdaságtudományi Egyetem)

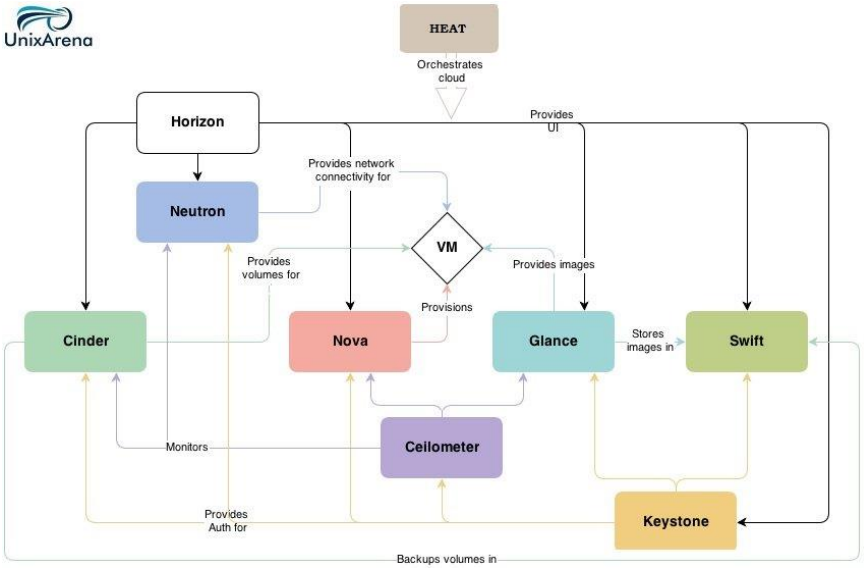
Hallgató: Koppány Péter

Trendek

A Network Function Virtualization (NFV) és a Software Defined Networking (SDN) a két meghatározó trend a jelenlegi hálózati és telekommunikációs világban. Ezen a hatások a tűzfalakat se kerülik el. A tűzfalak esetében is meg kell vizsgálni, hogy melyek azok az esetek, amikor a tradicionális – fizikai megvalósítás – a célravezető, vagy a virtuális megoldás. Továbbá a felhő alapú technológiák elterjedése miatt, várhatóan a virtuális tűzfalak is a felhőben lesznek elhelyezve tipikusan. Ilyen technológia például: Openstack vagy Vmware.

Openstack általánosságban

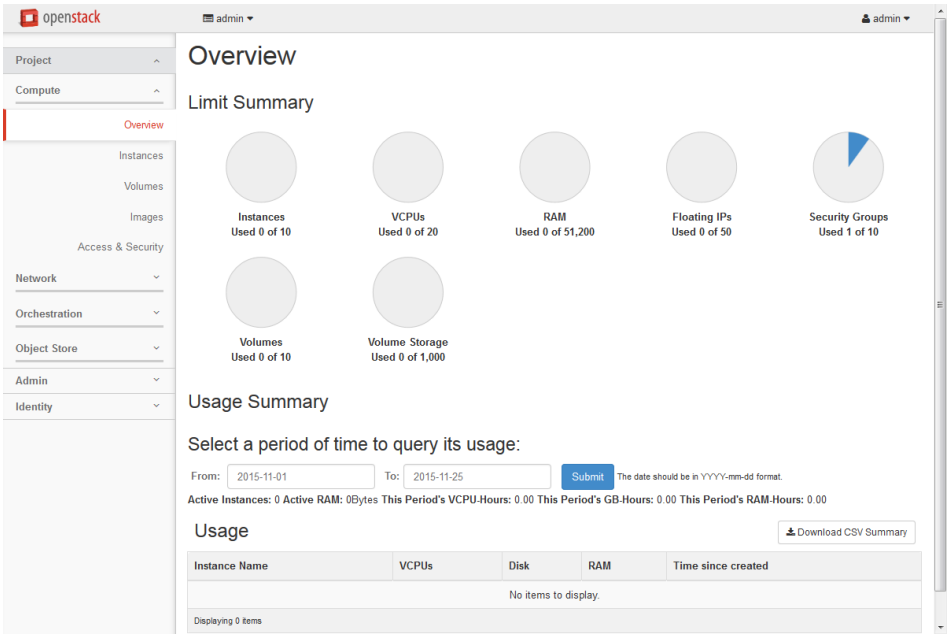
Az Openstack egy felhő keretrendszer, melynek segítségével virtuális erőforrásokat lehet menedzselni, pl virtuális gép, virtuális hálózat.



Kép 1 Openstack architektúra (forrás: https://steemitimages.com/0x0/https://res.cloudinary.com/hpiynhbhq/image/upload/v1514782734/wjaprleatv62wsmky24y.jpg)

Több különböző komponensből áll az Openstack:

- Glance: image fájlok kezelése
- Keystone: authentikációs szolgáltatás
- Neutron: hálózati menedzsment
- Nova: virtuális gépek kezelése
- Heat: automatikus infrastruktúra példányosaitás leíró fájlok alapján (stack)



Kép 2 Az Openstack webes felületének kezdőképernyője (forrás: https://docs.openstack.org/horizon/pike/_images/dashboard_project_tab.png)

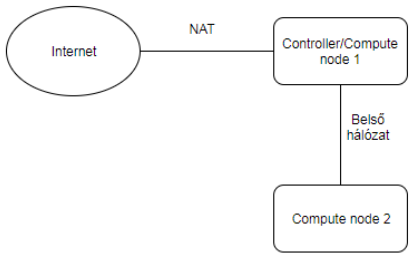
Az infrastruktúra két fő elemet tartalmaz:

- Contoller Node: központi vezérlőegység
- Compute Node: a virtuális gépek futtatásáért felelős elem.

Az egyes komponensek különböző kiegészítéseket is képesek befogadni, pl a Neutronnak van hálózati eszköz gyártókhoz kapcsolódó speciális kiegészítései.

Környezet felépítése

Korábbi munka során a tűzfallak tesztelésére létrehoztunk egy teszt környezetet. Két compute node lett kialakítva. Igy több féle teszt esetet lehet megvizsgálni.



Kép 3 Megvalósitott tesztkörnyezet

Tűzfalak általános jellemzői és választásának alap kritériumai

Meg kell vizsgálni első közelítésben az alábbi paramétereket:

- Milyen rétegben képes működni a tűzfal? L2..L7?
- Mekkora késleltetés generál a csomagfeldolgozás?
- Mekkora terhelést képes elviselni?
- Képes-e terhelés elosztásra?
- Milyen egyéb, hasznos funkciókkal rendelkezik, pl.:
    - SSL offloading
    - TCP SYN Proxy

A műszaki szempontokon felül van jónéhány egyéb tulajdonság is:

- Ár
- Beszerzési idő
- Telepítési idő
- Beszerelés: van-e speciális szerszám igény?
- Licensz kezelés az egyes funkciókhoz
- Speciális karbantartási igény?

F5 platform

Az F5 egy tűzfal gyártó cég, amely rendelkezik fizikai és virtuális tűzfalakkal is. Fő terméke a BIG-IP platform. Egy másik fő irányvonal a Viprion termékcsalád. A BIG-IQ rendszer szintén az F5 palettához tartozik és az egyik legfontosabb része a távoli licensz menedzsment.

Az F5 kiterjedt licenszelési megoldással rendelkezik:

https://f5.com/products/how-to-buy/simplified-licensing

Alkalmazásról alkalmazásra meg lehet választani, hogy szükség van-e rá. Az árazási modellje szerint már néhány alkalmazás megvásárlása után, akár hozzá lehet jutni a teljes F5 funkcionalitáshoz.

F5 automatikus konfigurálásához használható a cloud-init nevű, Linux alapú technológia. Ez azt jelenti, hogy egy ISO formátumú fájlként becsatolt virtuális CDROM meghajtó tartalmát a virtuális gép induláskor feldolgozza és az abban található beállítások alapján felkonfigurálja az adott virtuális gépet. Ilyen testre szabott beállítás pl. az IP cím és a hostname. Az Openstack és az Amazon rendelkezik saját cloud-init formátummal.

F5 Openstack integráció

Az Openstackel való könnyebb együttműködés elősegítés végett, született Openstack kiegészítés az F5 számára, itt érhető el:

https://clouddocs.f5.com/products/openstack/lbaasv2-driver/master/

A csomag lehetővé teszi, hogy az F5 együttműködjön az Openstack Load-Balancer-as-a-Service szolgáltatásával.

Összehasonlítás

Az alábbi táblázat szemlélti az irodalomkutatási eredményeket:

	Előny	**Hátrány**
Fizikai	Sebesség Kapacitás FPGA rásegítés	Ár Fejlesztési korlátok Beszerelés nehézsége Speciális hardver Beszerzés
Virtuális	Könnyű telepités Azonnal elérhető Könnyű a cloud technológiákkal való együttműködés	Erőforrás

Összegzés

Nem lehet teljesen egyértelműen rámondani, hogy melyik konfiguráció a „jobb”. Egy induló vállalkozás eseten a virtuális megoldás lényegesebben olcsóbb lehet, és könnyebben hozzáférhető is. Egy meglevő nagy vállalat forgalmi igénye esetén a fizikai megvalósítás több előnnyel járhat a rendkívül magas feldolgozási képessége miatt. Mindig meg kell vizsgálni az igényeket és az alapján dönteni. Ez a munka segít egy képet adni, hogy miket kell figyelembe venni.

2018. június 25.

Szakmai önéletrajz

Leiter Ákos

Iskolai végzettség:

Budapesti Műszaki és Gazdaságtudományi Egyetem – Informatikai Tudományok Doktori Iskola (2016 februártól)

IP alapú mobilitáskezelési eljárások kutatása és fejlesztése

Budapesti Műszaki és Gazdaságtudományi Egyetem - Mérnök Informatikus MSC - Hálózatok és szolgáltatások szakirány (2015 június)

Diplomaterv címe: Proxy Mobile IPv6 protokoll LTE/EPC rendszerekben
A BSC-n elkezdett témát, az IP alapú mobilitást folytattam. A munka során vizsgáltam a témában írt RFC és RFC draftok működését, implementációjának lehetőségeit. Az LMA, mint non-3GPP hozzáférés kezelését végző elem és a PCRF közötti interfész megvalósíthatóságának vizsgálta. A diplomaterv PMIPv6 alapú Flow Binding megvalósítása linuxos környezetben shell scriptek segítségével.

Kari TDK Dicséret (2014): Leiter Ákos: Folyam szintű és operátor-központú dinamikus mobilitás-kezelés megvalósítása Proxy Mobile IP segítségével
Konzulens: dr. Bokor László
Mesterpróba 1. helyezés (2015): Akos Leiter: A Virtual Testbed for Analysis and Design of Advanced Network-Based Mobility Extensions
Konzulens: dr. Bokor László

Budapesti Műszaki és Gazdaságtudományi Egyetem - Mérnök Informatikus BSC - Mobil infokommunikációs szakirány (2013 január)

Szakdolgozat címe: A Proxy Mobile IPv6 (PMIPv6) protokoll funkcionális és teljesítményvizsgálata.
A szakirányon a mobilinformmunikáció működésének alapjaival lehetett megismerkedni, mind a rádiós, mind a protokollfelépítésekkel.

Egyéb,nem a szakmai törzsanyag keretében hallgatott tantárgyak:

- IPv6 alapú hálózatok (ACL, DNS, OSPF, EIGRP, BGP, Multicast IPv6 környezetben)
- Linux programozás (C/C++ alapú programozás Linux környezetben - GCC,G++,Qt)
- Virtualizációs technikák és eljárások (VMWare ESXi, Xen)
- Számvitel és pénzügyek alapjai

Munkahelyek

2014-tól – jelenleg: Ericsson Magyarország, szoftverfejlesző mérnök
2011-2014: T- Systems Magyarország, gyakornok

Nyelvtudás:

- Angol felsőfok írásban és szóban

Jogosítvány: B kategória