Infrastrutture virtuali

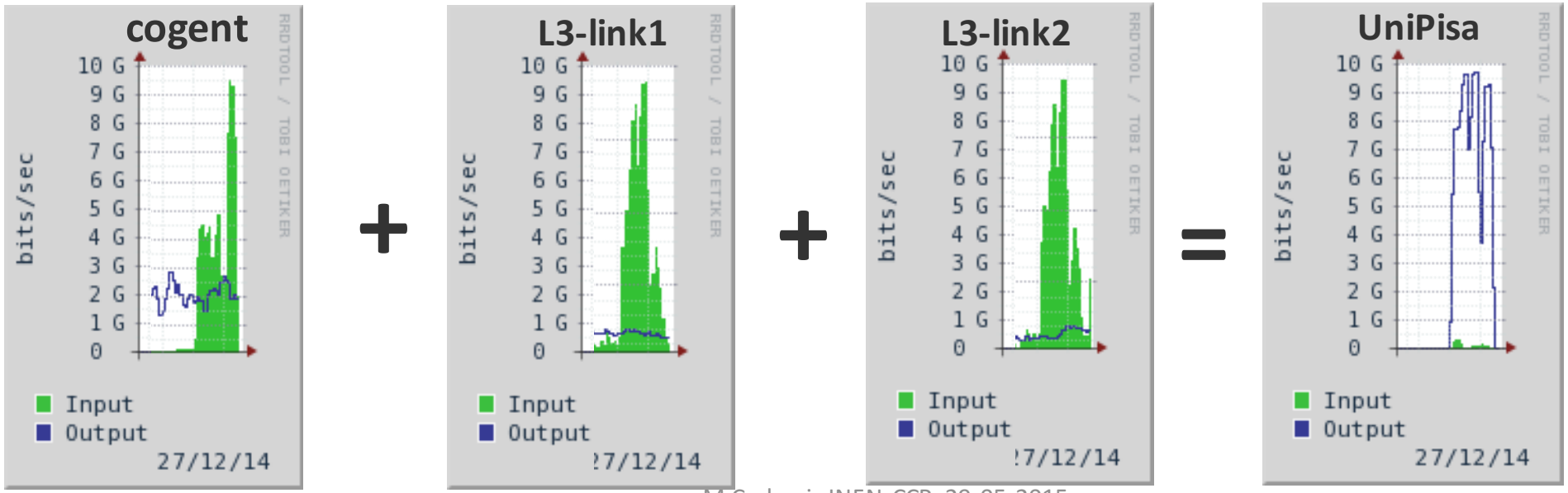
by M.Carboni

… la questione della sicurezza

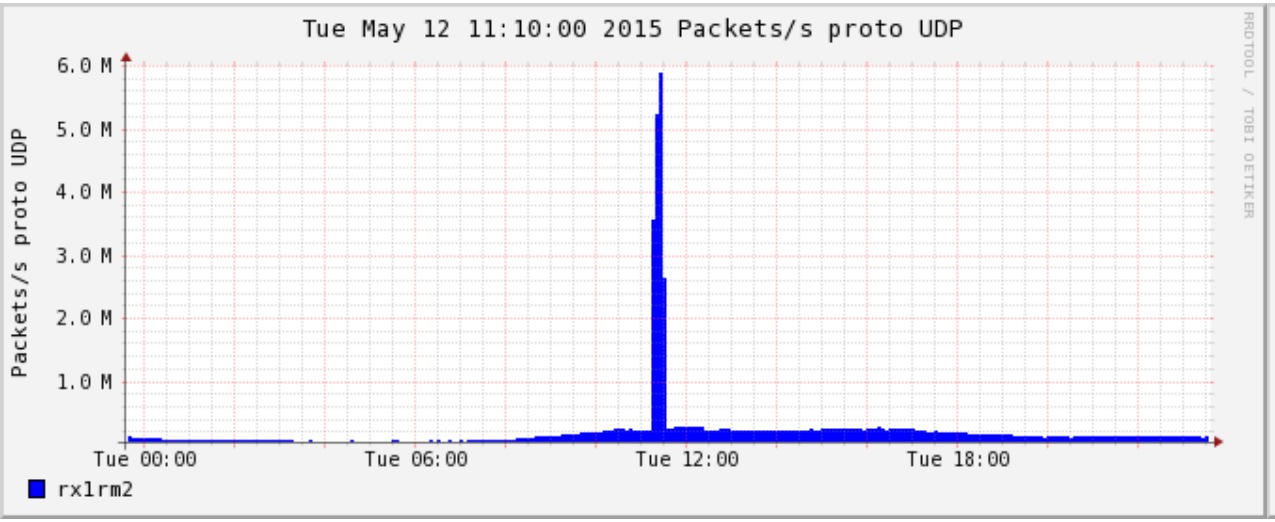
DDoS verso UniPisa

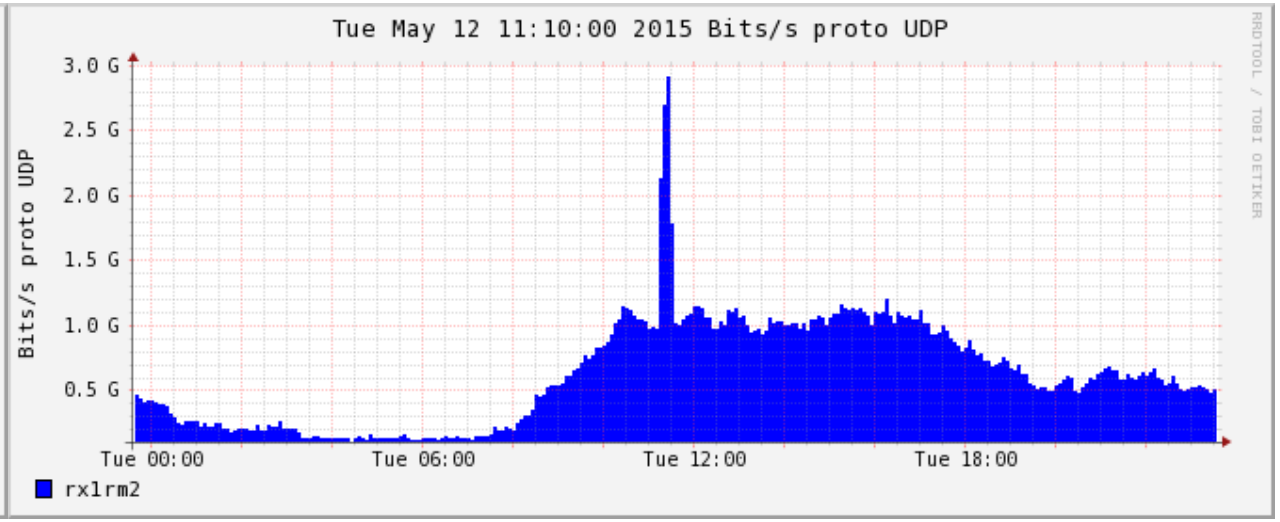
I potenziali effetti di rete di attacco su utenza a 10G 27/12/2014

Sorgente	Destinazione	Traffico	% sul totale: 2.9 TB
CHINA169-BACKBONE(AS4837)	UNI-Pisa	251.36 GB	8.45%
CHINANET-BACKBONE(AS4134)	UNI-Pisa	150.61 GB	5.06%
COMCAST-7922(AS7922)	UNI-Pisa	109.69 GB	3.69%
CHARTER-NET-HKY-NC(AS20115)	UNI-Pisa	41.97 GB	1.41%
SHAW(AS6327)	UNI-Pisa	38.06 GB	1.28%
CTTNET(AS9394)	UNI-Pisa	28.8 GB	0.97%
Telemar(AS7738)	UNI-Pisa	23.89 GB	0.80%
UUNET(AS701)	UNI-Pisa	22.93 GB	0.77%
ROADRUNNER-WEST(AS20001)	UNI-Pisa	22.92 GB	0.77%
CABLE-NET-1(AS6128)	UNI-Pisa	21.48 GB	0.72%
Global(AS18881)	UNI-Pisa	20.5 GB	0.69%
Brasil Telecom S/A(AS8167)	UNI-Pisa	20.25 GB	0.68%
COGECOWAVE(AS7992)	UNI-Pisa	19.86 GB	0.67%
SCRR-10796(AS10796)	UNI-Pisa	19.5 GB	0.66%



DDoS da UniRoma1



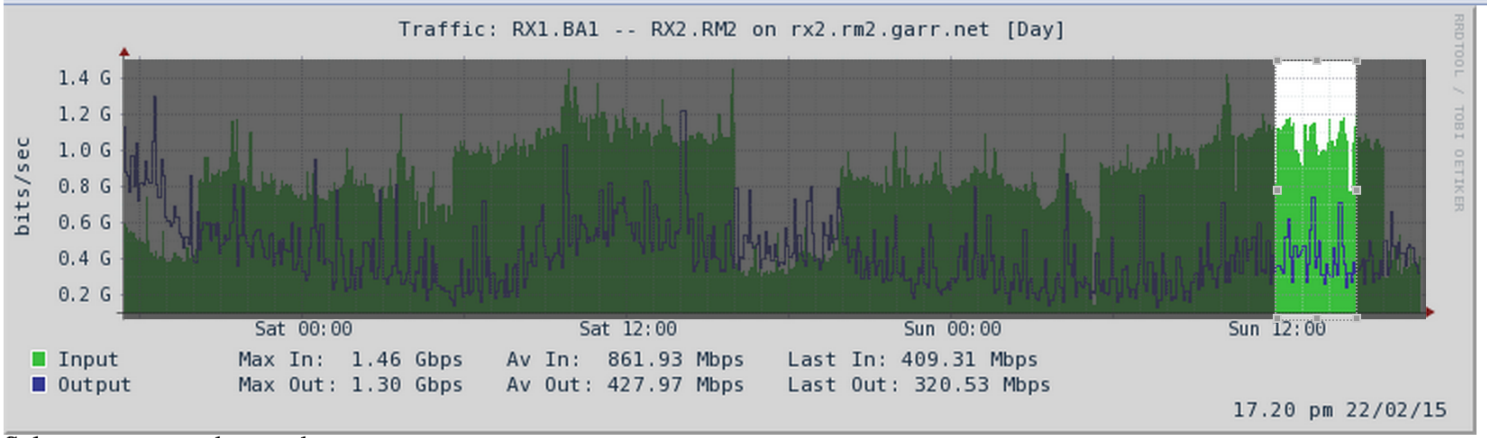



```
** nfdump -M /data/nfsen/profiles-data/live/rx1rm2  -T  -R 2015/05/12/nfcapd.201505121110:2015/05/12/nfcapd.201505121130 -n 10 -s ip/flows
nfdump filter:
proto UDP
Top 10 IP Addr ordered by flows:
Date first seen          Duration Proto            IP Addr    Flows(%)      Packets(%)        Bytes(%)        pps      bps   bpp
2015-05-12 11:10:25.440  1500.830 any       193.206.141.46   10704( 7.7)    10.7 M( 0.2)     1.1 G( 0.3)     7136    5.8 M   101
2015-05-12 11:10:26.630  1499.540 any       194.119.192.34    6195( 4.5)     6.2 M( 0.1)   679.8 M( 0.2)     4131    3.6 M   109
2015-05-12 10:02:47.600  5613.420 any          193.205.5.2    6185( 4.5)    18.2 M( 0.3)    11.1 G( 2.8)     3245   15.9 M   610
2015-05-12 11:17:14.850  1104.100 any      151.100.8.114     2736( 2.0)     4.9 G(94.2)   215.4 G(54.9)     4.5 M    1.6 G    43
2015-05-12 11:10:26.730  1497.740 any            8.8.8.8     1123( 0.8)     1.2 M( 0.0)   126.2 M( 0.0)      777  674023   108
2015-05-12 11:10:26.560  1545.810 any      146.48.81.102     1018( 0.7)     1.9 M( 0.0)   153.2 M( 0.0)     1238  792832    79
2015-05-12 11:04:38.410  1894.070 any      150.217.15.245     969( 0.7)     3.8 M( 0.1)     2.7 G( 0.7)     2031   11.5 M   707

Summary: total flows: 138378, total bytes: 392.1 G, total packets: 5.2 G, avg bps: 1.1 M, avg pps: 1852, avg bpp: 74
Time window: 2015-04-09 18:15:33 - 2015-05-12 11:36:25
Total flows processed: 992276, Blocks skipped: 0, Bytes read: 119539320
Sys: 0.435s flows/second: 2276212.2  Wall: 0.433s flows/second: 2287246.2
```

151.100.8.114 2736(2.0) 4.9 G(94.2) 215.4 G(54.9) 4.5 M 1.6 G

Nfsen -- Logged in as: *(admin)* Logout



Select an area on the graph:
Start Date: Sun Feb 22 2015 11:35:59 GMT+0100 (CET)
End Date: Sun Feb 22 2015 14:31:29 GMT+0100 (CET)

get flow details | get flow list | get flow list no net | get sites details

Date first seen	Proto	Src IP Addr:Port		Dst IP Addr:Port	Flags	Src AS	Dst AS	Packets	Input	Output	Bytes
2015-02-22 11:35:04.690	TCP	207.46.13.35:2897	->	193.204.68.200:80	.A...F	8075	137	1000	791	809	44000
2015-02-22 11:34:06.400	TCP	90.147.102.214:57472	->	124.228.91.53:7010	....S.	137	4134	1000	809	825	940000
2015-02-22 11:34:06.400	TCP	90.147.102.214:15410	->	124.228.91.53:7010	....S.	137	4134	2000	809	825	1.9 M
2015-02-22 11:34:06.390	TCP	90.147.102.214:39944	->	124.228.91.53:7010	....S.	137	4134	1000	809	825	940000
2015-02-22 11:34:06.390	TCP	90.147.102.214:31465	->	124.228.91.53:7010	....S.	137	4134	1000	809	825	940000
2015-02-22 11:34:06.390	TCP	90.147.102.214:27539	->	124.228.91.53:7010	....S.	137	4134	1000	809	825	940000
2015-02-22 11:34:06.390	TCP	90.147.102.214:9863	->	124.228.91.53:7010	....S.	137	4134	1000	809	825	940000
2015-02-22 11:34:06.370	TCP	130.246.179.248:51383	->	212.189.205.108:54730	.A....	786	137	13000	791	809	788000
2015-02-22 11:34:06.340	TCP	90.147.102.214:59248	->	124.228.91.53:7010	....S.	137	4134	1000	809	825	940000
2015-02-22 11:34:06.340	TCP	90.147.102.214:2241	->	124.228.91.53:7010	....S.	137	4134	2000	809	825	1.9 M
2015-02-22 11:34:06.330	TCP	90.147.102.214:18521	->	124.228.91.53:7010	....S.	137	4134	1000	809	825	940000
2015-02-22 11:34:06.330	TCP	90.147.102.214:41548	->	124.228.91.53:7010	....S.	137	4134	1000	809	825	940000
2015-02-22 11:34:06.320	TCP	90.147.102.214:16386	->	124.228.91.53:7010	....S.	137	4134	2000	809	825	1.9 M
2015-02-22 11:34:06.320	TCP	90.147.102.214:51939	->	124.228.91.53:7010	....S.	137	4134	1000	809	825	940000
2015-02-22 11:34:06.320	TCP	195.154.226.5:35432	->	160.97.47.30:443	.AP...	12876	137	1000	825	809	599000
2015-02-22 11:34:06.320	TCP	90.147.102.214:17181	->	124.228.91.53:7010	....S.	137	4134	1000	809	825	940000
2015-02-22 11:34:06.320	TCP	90.147.102.214:53409	->	124.228.91.53:7010	....S.	137	4134	1000	809	825	940000
2015-02-22 11:34:06.320	TCP	90.147.102.214:30853	->	124.228.91.53:7010	....S.	137	4134	1000	809	825	940000
2015-02-22 11:34:06.310	TCP	90.147.102.214:43856	->	124.228.91.53:7010	....S.	137	4134	1000	809	825	940000
2015-02-22 11:34:06.310	UDP	71.196.10.177:26085	->	193.204.74.205:20706	.....	7922	137	1000	825	809	135000
2015-02-22 11:34:06.300	TCP	193.204.186.180:3389	->	95.78.127.198:3772	.AP...	137	42116	1000	809	825	59000
2015-02-22 11:34:06.300	TCP	192.167.60.16:48485	->	62.149.152.152:995	.A....	137	31034	18000	809	825	1.1 M
2015-02-22 11:34:06.290	TCP	90.147.102.214:29652	->	124.228.91.53:7010	....S.	137	4134	1000	809	825	940000
2015-02-22 11:34:06.280	TCP	90.147.102.214:48455	->	124.228.91.53:7010	....S.	137	4134	1000	809	825	940000
2015-02-22 11:34:06.280	TCP	90.147.102.214:37605	->	124.228.91.53:7010	....S.	137	4134	1000	809	825	940000
2015-02-22 11:34:06.260	TCP	90.147.102.214:20519	->	124.228.91.53:7010	....S.	137	4134	1000	809	825	940000
2015-02-22 11:34:06.250	TCP	78.40.168.161:60817	->	81.74.229.37:80	.A....	35110	3269	1000	809	825	44000

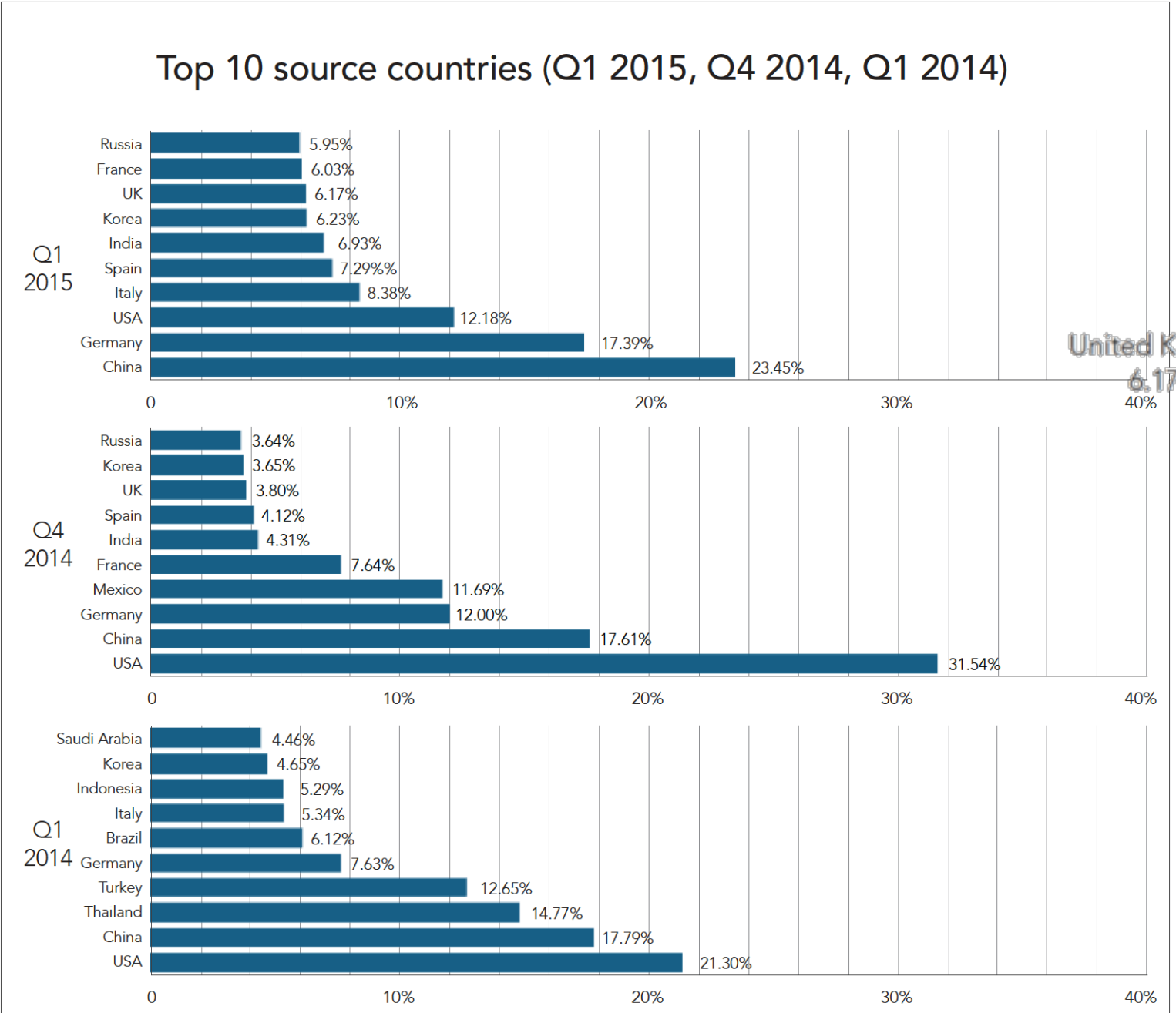
Technical Details Behind a 400Gbps NTP Amplification DDoS Attack

13 Feb 2014 by Matthew Prince.

http://cert.garr.it/documentazione/articoli-tecnici/25-articolo-ntp-ddos

ASN	Network	Count
9808	CMNET-GD Guangdong Mobile Communication Co.Ltd.	136
4134	CHINANET-BACKBONE No.31,Jin-rong Street	116
16276	OVH OVH Systems	114
4837	CHINA169-BACKBONE CNCGROUP China169 Backbone	81
3320	DTAG Deutsche Telekom AG	69
39116	TELEHOUSE Telehouse Inter. Corp. of Europe Ltd	61
10796	SCRR-10796 - Time Warner Cable Internet LLC	53
6830	LGI-UPC Liberty Global Operations B.V.	48
6663	TTI-NET Euroweb Romania SA	46
9198	KAZTELECOM-AS JSC Kazakhtelecom	45
2497	IIJ Internet Initiative Japan Inc.	39
3269	ASN-IBSNAZ Telecom Italia S.p.a.	39
9371	SAKURA-C SAKURA Internet Inc.	39
12322	PROXAD Free SAS	37
20057	AT&T Wireless Service	37
30811	EPiServer AB	36
137	ASGARR GARR Italian academic and research network	34
209	ASN-QWEST-US NOVARTIS-DMZ-US	33
6315	XMISSION - XMission, L.C.	33
52967	NT Brasil Tecnologia Ltda. ME	32
4713	OCN NTT Communications Corporation	31
56041	CMNET-ZHEJIANG-AP China Mobile communications corporation	31
1659	ERX-TANET-ASN1 Tiawan Academic Network (TANet) Information Center	30
4538	ERX-CERNET-BKB China Education and Research Network Center	30

CLOUDFLARE



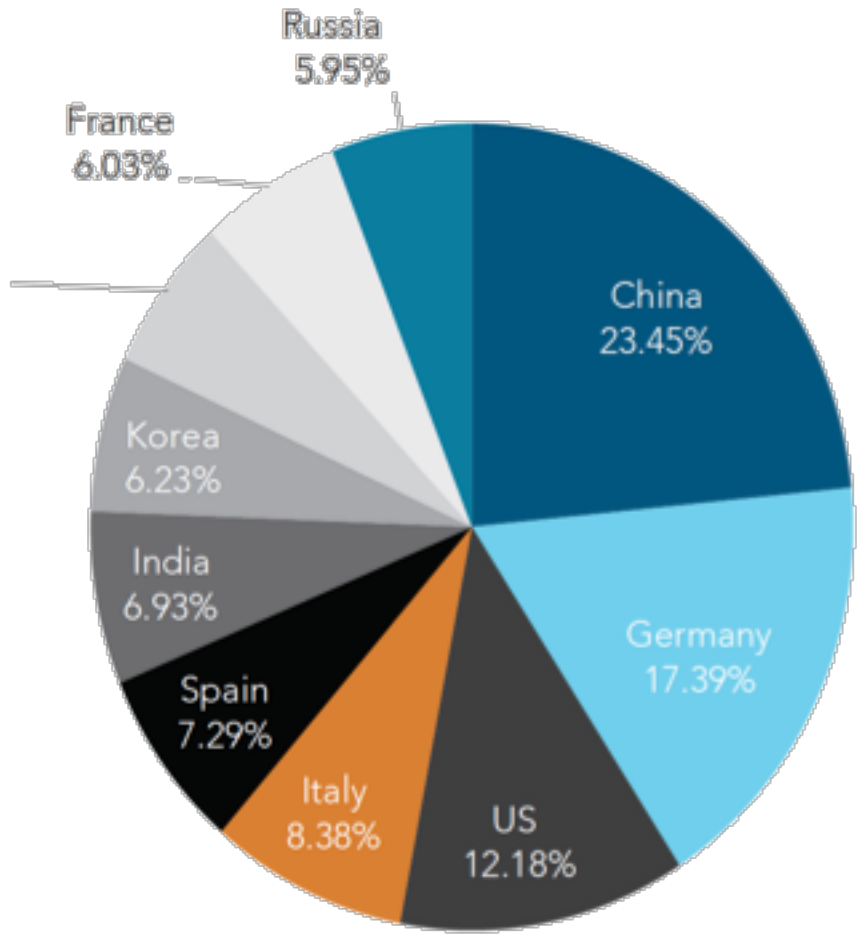


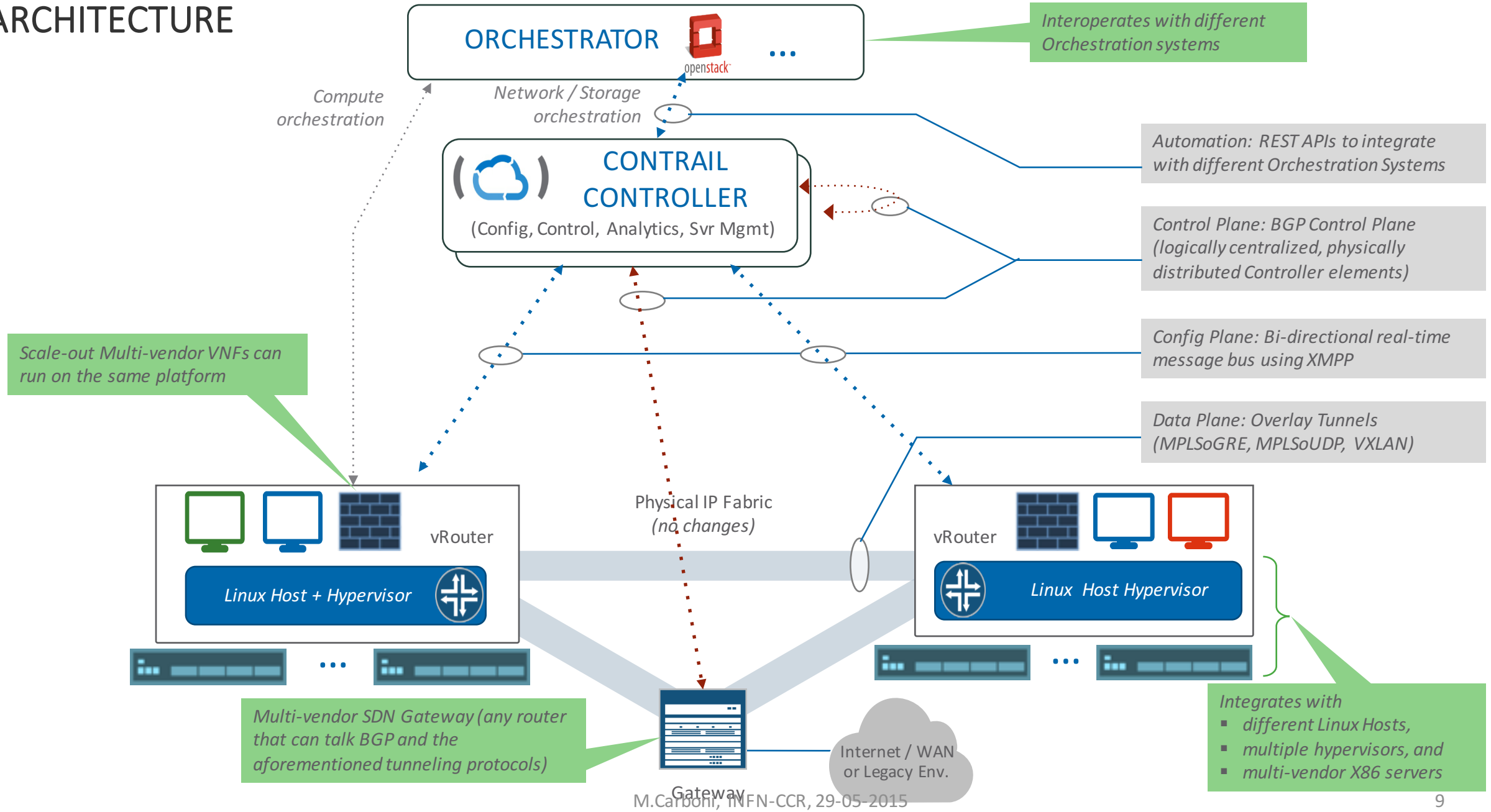
Figure 1-6: China, Germany and the US are consistently among the top 10 sources for non-spoofed attacking IPs

SDN: Contrail, NFV, vCPE

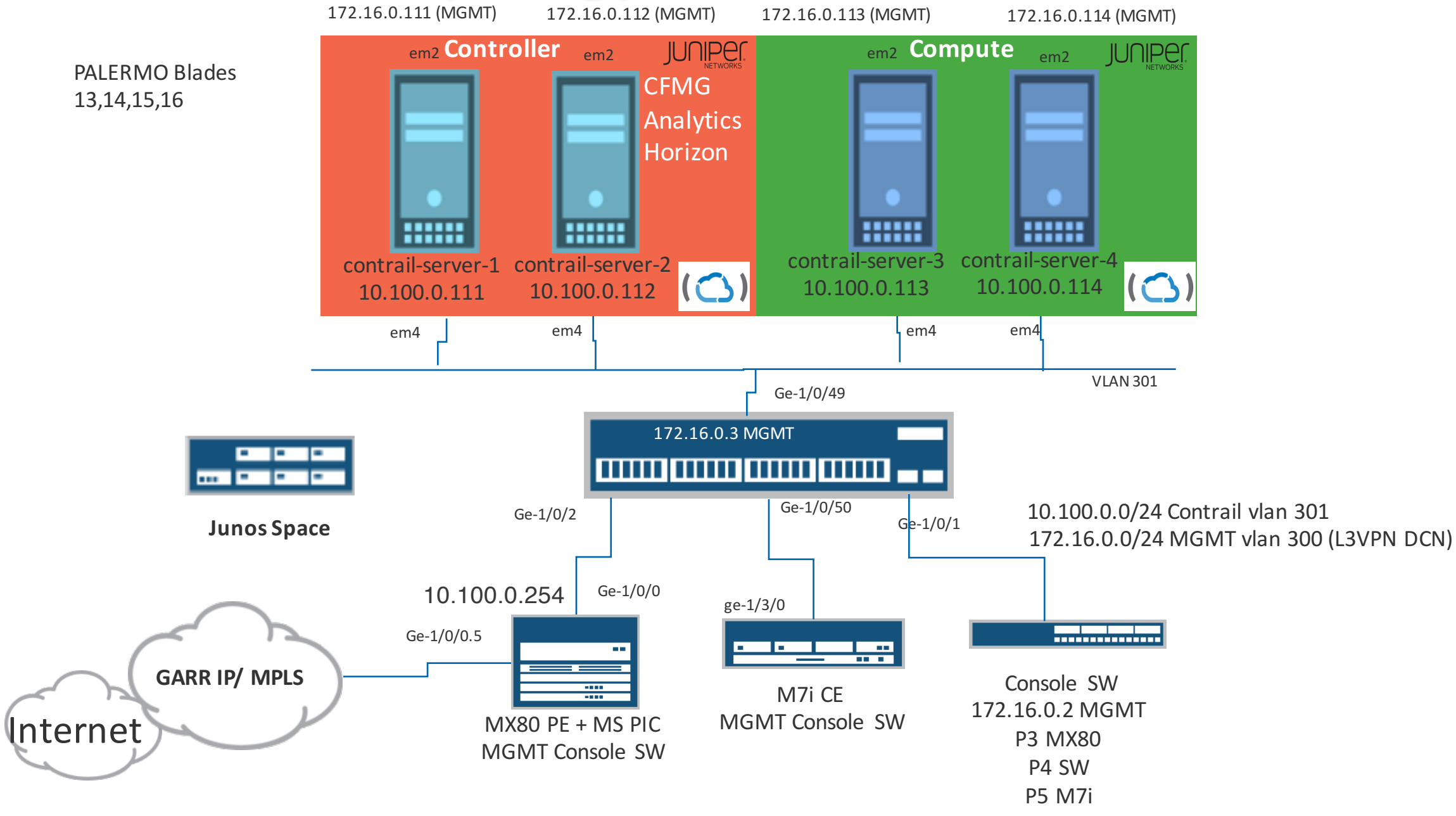
Risultati preliminari

G.Viola, C.Valli, M.Marletta, I.Tomic

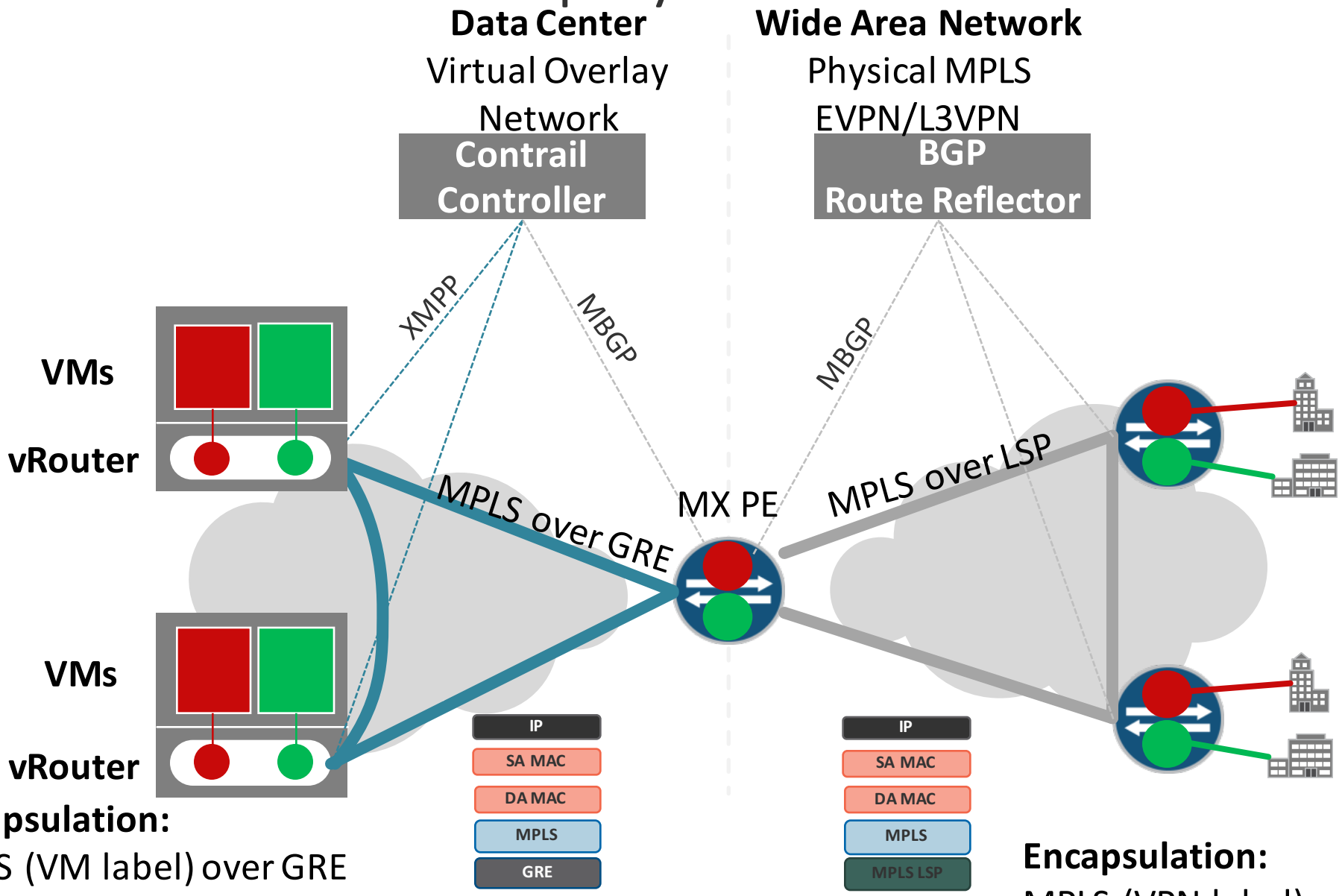
CONTRAIL (MULTI-VENDOR) SW ARCHITECTURE



vCPE POC LAB Topology



Virtual and physical infrastructure



Encapsulation:
MPLS (VM label) over GRE
MPLS over UDP
Or VXLAN

Encapsulation:
MPLS (VPN label) over LSP
(LDP or RSVP or both)

vCPE, le scuole e non solo

vCPE Services

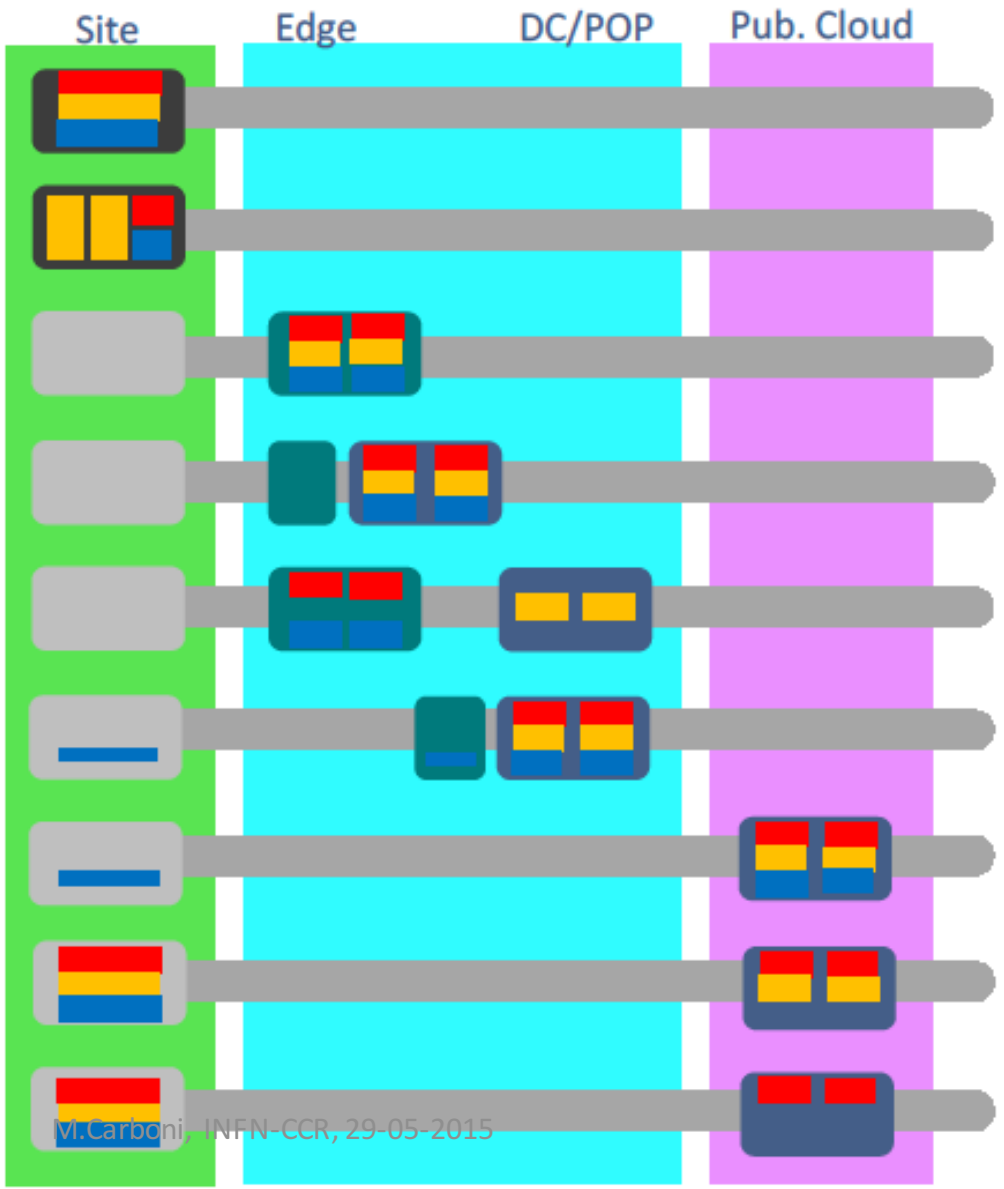
- **Infrastructure - IaaS**
- **Unified Threat Management (UTM)** (Mainly can be considered for the Schools Project)
  - Antivirus – AVaaS
  - Antispam – ASaaS
  - Stateful FW - FWaaS
  - Content filtering - CFaaS
  - Parental control/ URL filtering – UFaaS
- **Public and Private Web Services with DDoS protection**
  - Advanced Firewall/NAT
  - Remote Access using SSL VPN technologies
  - Centralized WLAN Controller
  - VoIP SIP Gateway/PBX

- **Virtualized services can have the following characteristics:**
  - L2 or L3 sCPE/Access Network
  - Managed Enterprise vCPE Service
  - Customer Traffic over IPv4 and IPv6
  - L3VPNs
  - Per-customer for Enterprise vCPE
  - Shared-service for Enterprise vCPE
  - Direct Internet Access
  - NAT service
  - Implemented in PE (MS-MPC, MS-PIC)
  - Implemented in Service-Chain (VNF, e.g. Firefly Perimeter)
  - Other VNFs
  - Layer 2 Service-Chains
  - Layer 3 Service-Chains

vCPE Models and Architecture

There are three general vCPE concepts or models of implementation:

- **On Site**
  - Bare Metal
  - VMs
- **Centralized**
  - L2 Agg.
    - **PE vCPE**
    - **Tethered vCPE**
    - **Hybrid vCPE**
  - L3 Agg.
    - **DC vCPE**
    - OTT vCPE
- **Mixed**
  - CPE + Cloud Services
  - CPE + Cloud Management



White label CPE HW
Open source or commercial SW

Distributed services (Security / Compliance, WAN optimization)

vCPE = Routing instance in PE
Incremental, Simple

vCPE as a VNF in dedicated host
Phys./Virt. stitching on PE

Basic vCPE on PE and service chaining toward vServices

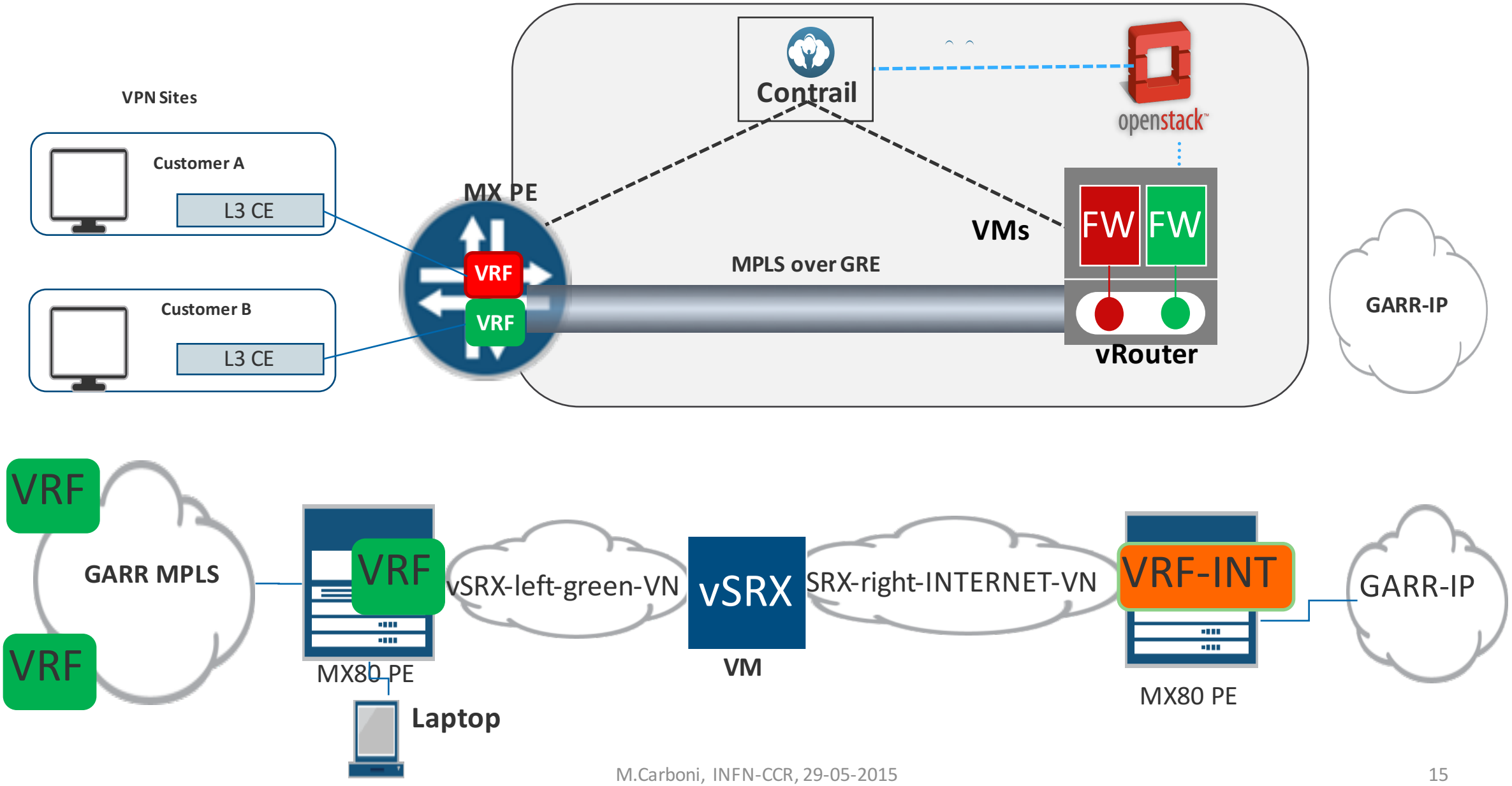
L3 Tunnels (eg. Ipsec) can be optimized on DC gateway

Overlay business services (NSP provides only Internet connectivity)

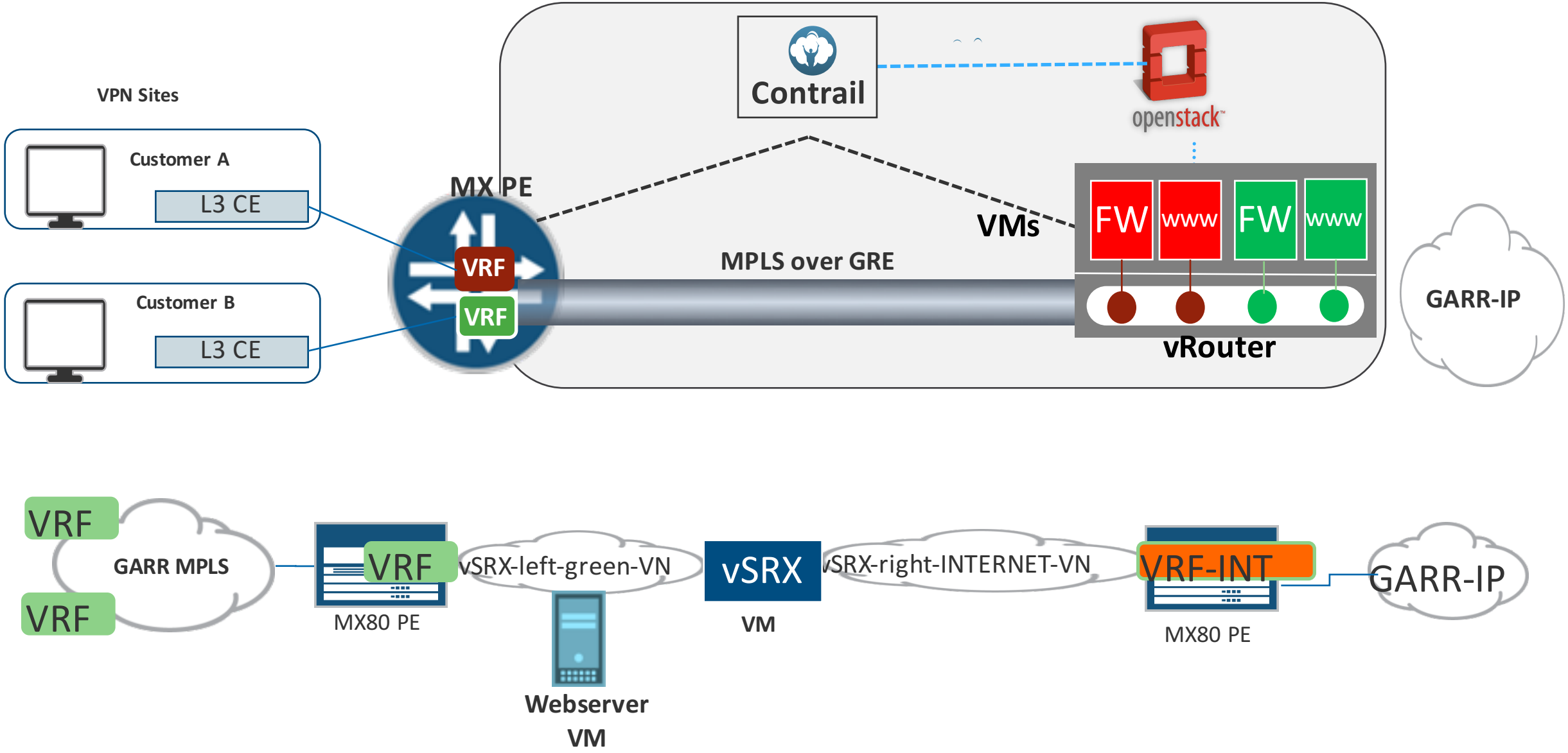
Cloud VAS (eg. Security)

Eg, Cisco Meraki (LAN Mgt from Public Cloud)

Use Case: vCPE

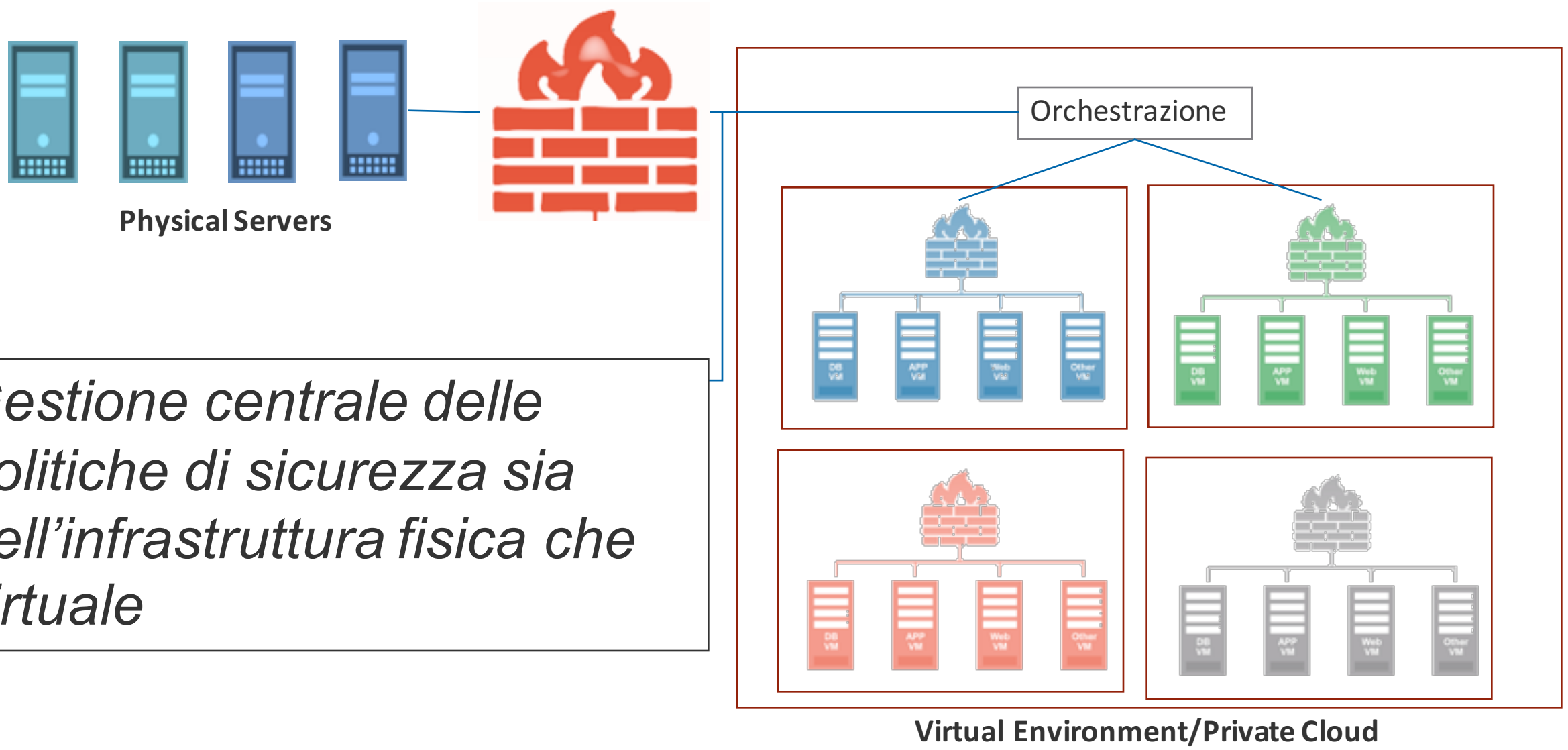


Use Case: vCPE + Web Hosting



Ulteriori casi d’uso

Use Case: Private or Hybrid Cloud

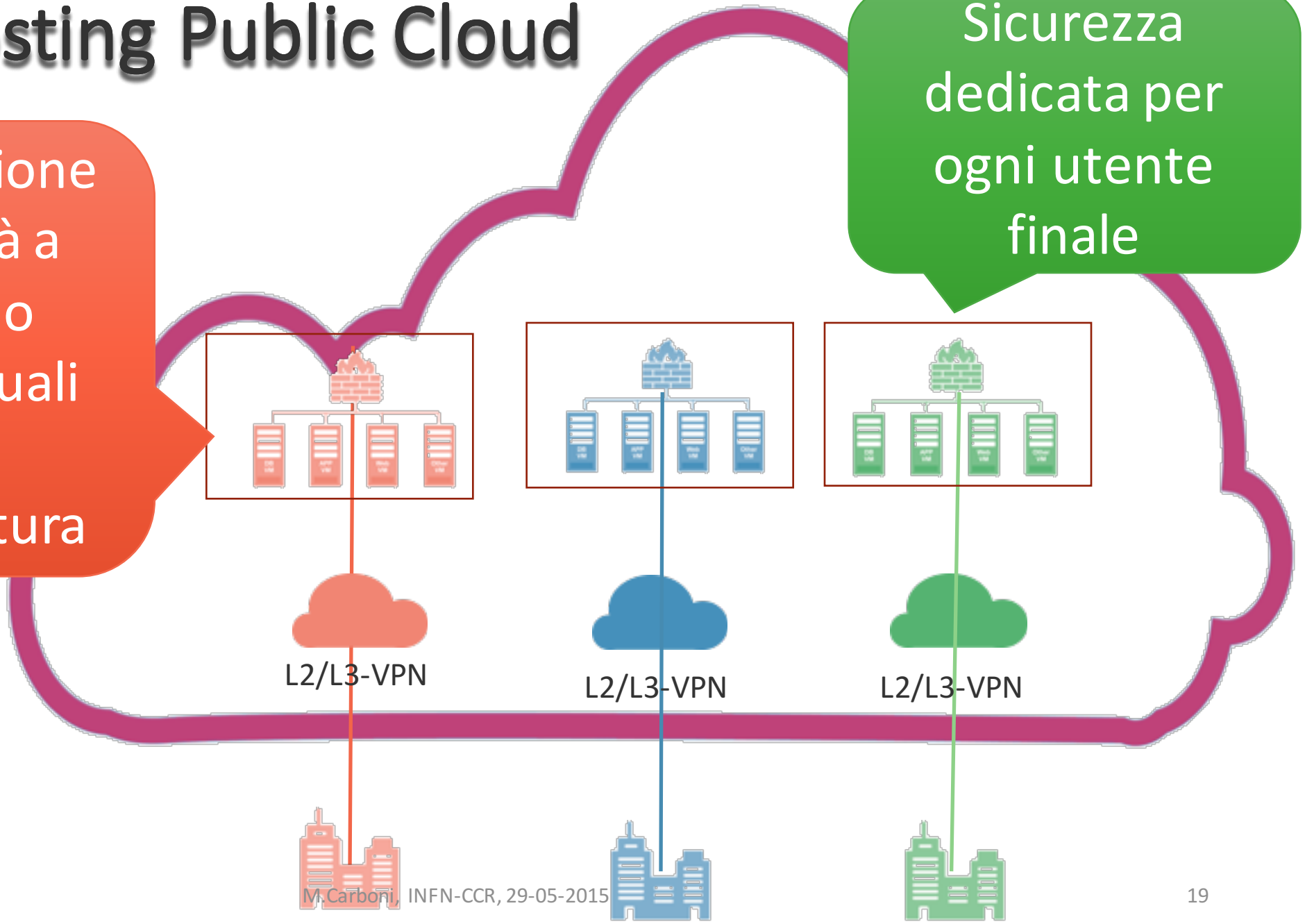


Gestione centrale delle politiche di sicurezza sia dell'infrastruttura fisica che virtuale

Use Case: Hosting Public Cloud

Fornire protezione e connettività a quanti hanno macchine virtuali ospitate nell'infrastruttura

Sicurezza dedicata per ogni utente finale



Considerazioni e prossimi passi

- La virtualizzazione sta offrendo la possibilità di concentrare all'interno del data center alcuni dei servizi di rete prima su ferro
- Molti vendor stanno commercializzando VM in grado d'implementare le funzioni di rete:
  - firewall, antivirus, ips, content-filtering, ecc.
- I possibili casi d'uso possono avere ricadute in diversi contesti:
  - scuole, hosting, data center consolidation, ecc
- Verificare la robustezza complessiva mediante casi d'uso
  - puntiamo verso un ambiente di pre-produzione ad uso interno
- Realizzare una configurazione HA su due site sia per i servizi che per il controller