WORKSHOP GARR 2022

NET MAKERS

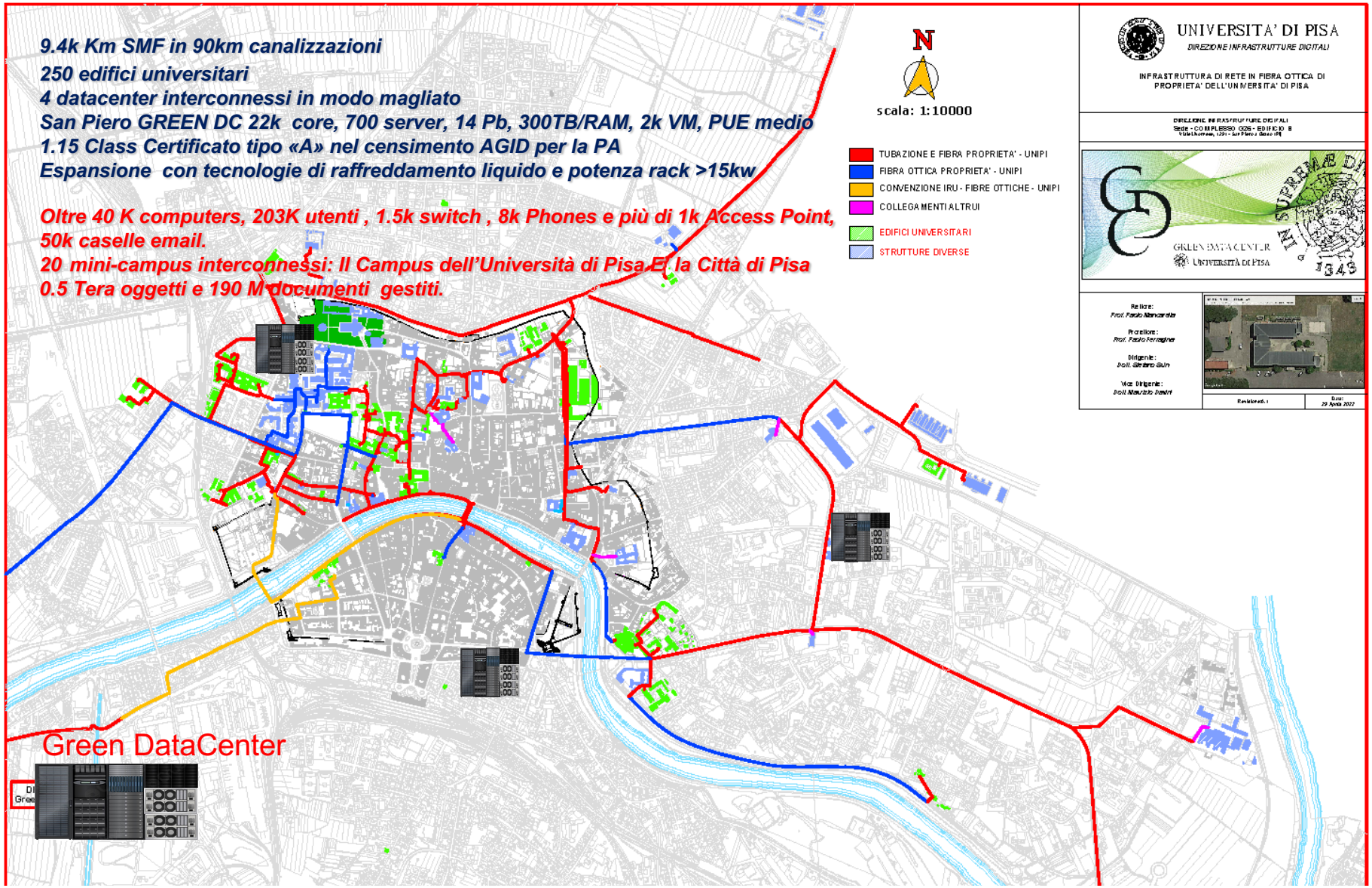
Una LAN su scala metropolitana: aspetti di progettazione e sicurezza

Stefano Suin

Università di Pisa

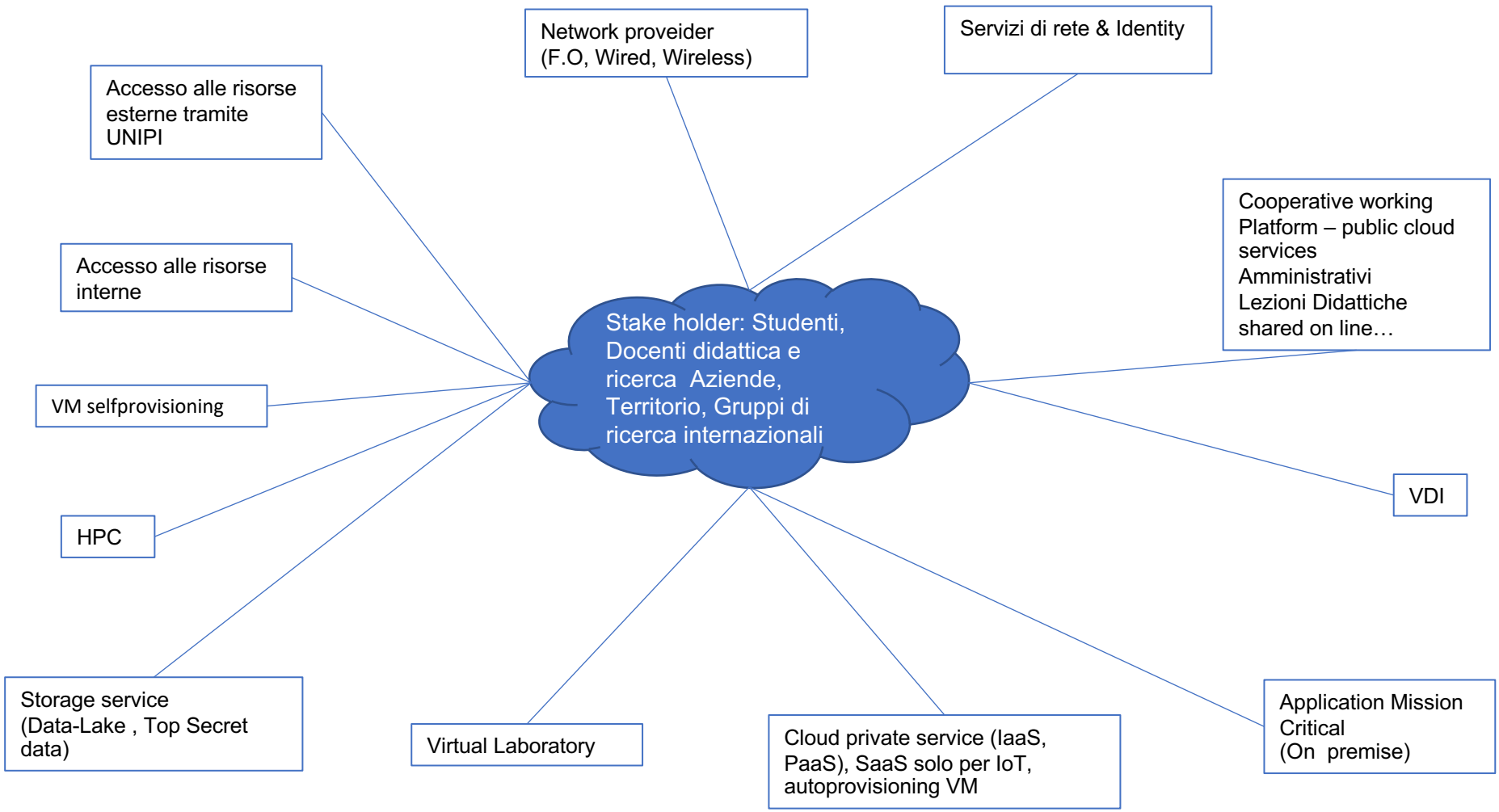
9.4k Km SMF in 90km canalizzazioni
250 edifici universitari
4 datacenter interconnessi in modo magliato
San Piero GREEN DC 22k core, 700 server, 14 Pb, 300TB/RAM, 2k VM, PUE medio 1.15 Class Certificato tipo «A» nel censimento AGID per la PA
Espansione con tecnologie di raffreddamento liquido e potenza rack >15kw

Oltre 40 K computers, 203K utenti , 1.5k switch , 8k Phones e più di 1k Access Point, 50k caselle email.
20 mini-campus interconnessi: Il Campus dell'Università di Pisa E la Città di Pisa
0.5 Tera oggetti e 190 M documenti gestiti.



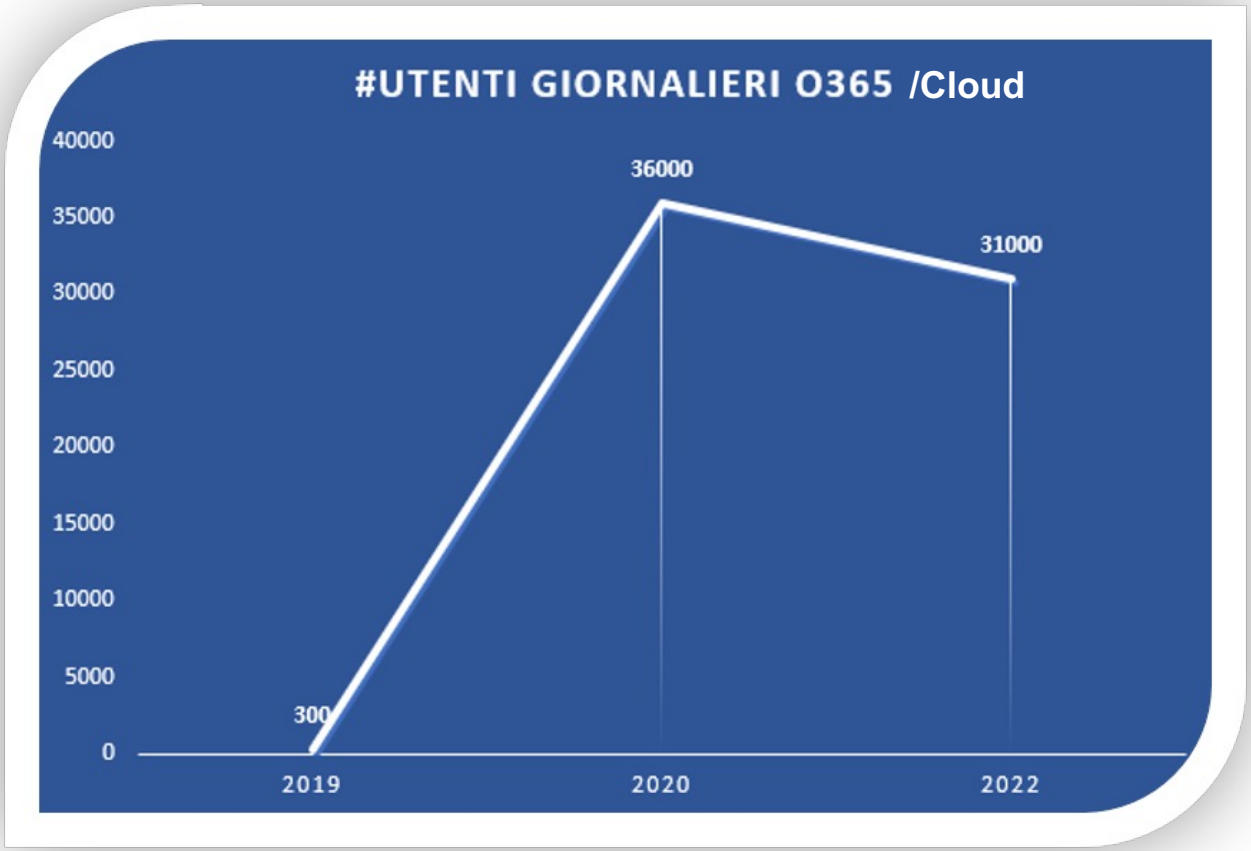
Un datacenter brandpisanizzato

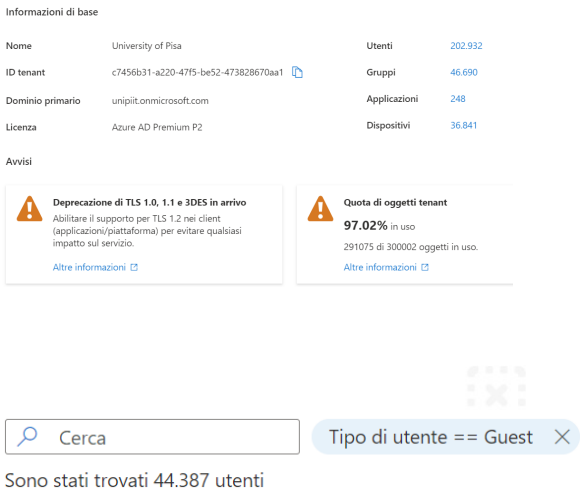
Servizi Unipi



Uso dei servizi cloud e del cooperative working

Digitalizzaione (+1%) durante pandemia (+10000%, fattore 100) e dopo (-15/20%)

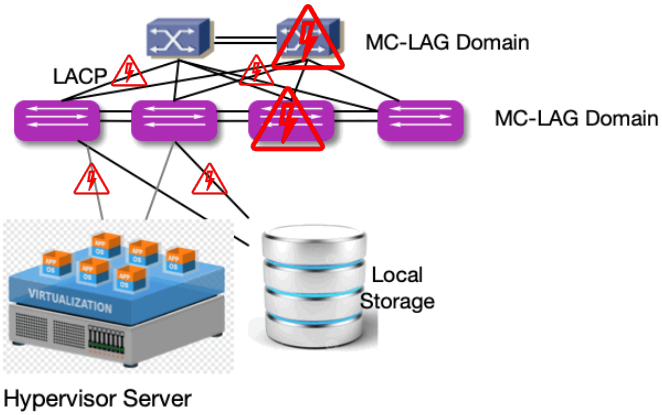


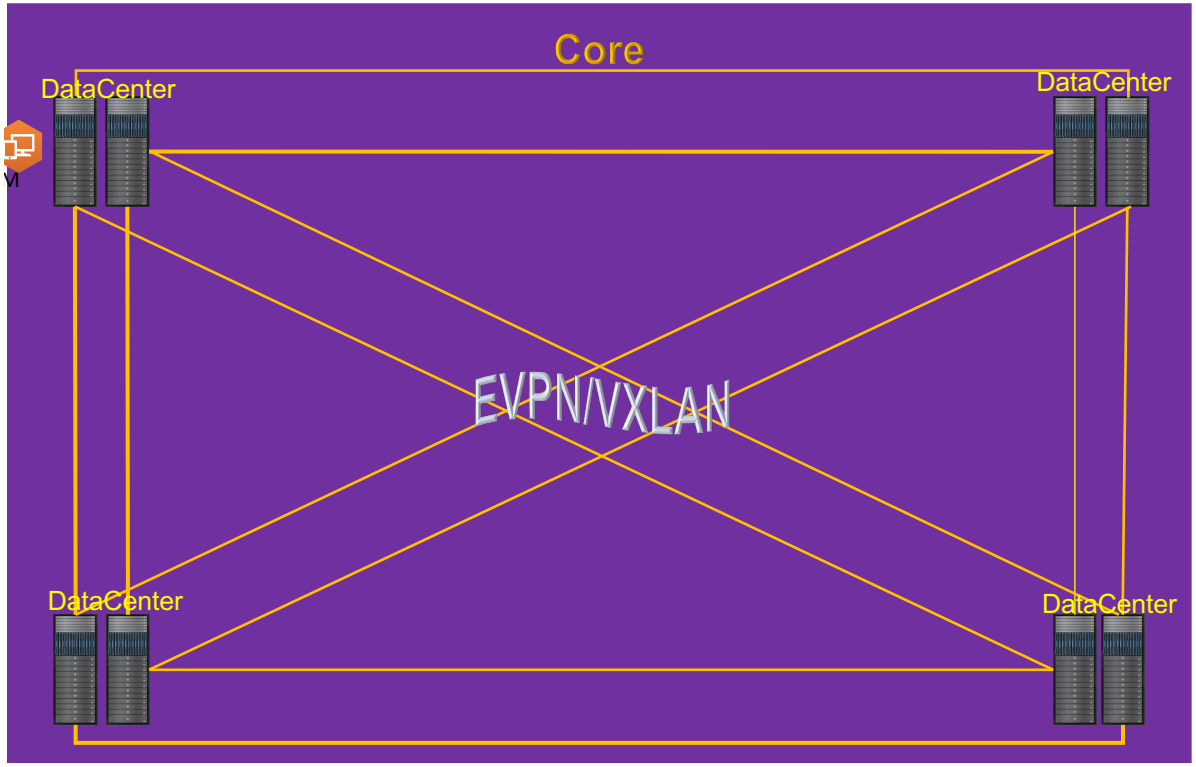


FabricNet: Una semplice e robusta architettura service oriented

All active

POD - Point of Deliver
Storage,Computing,network

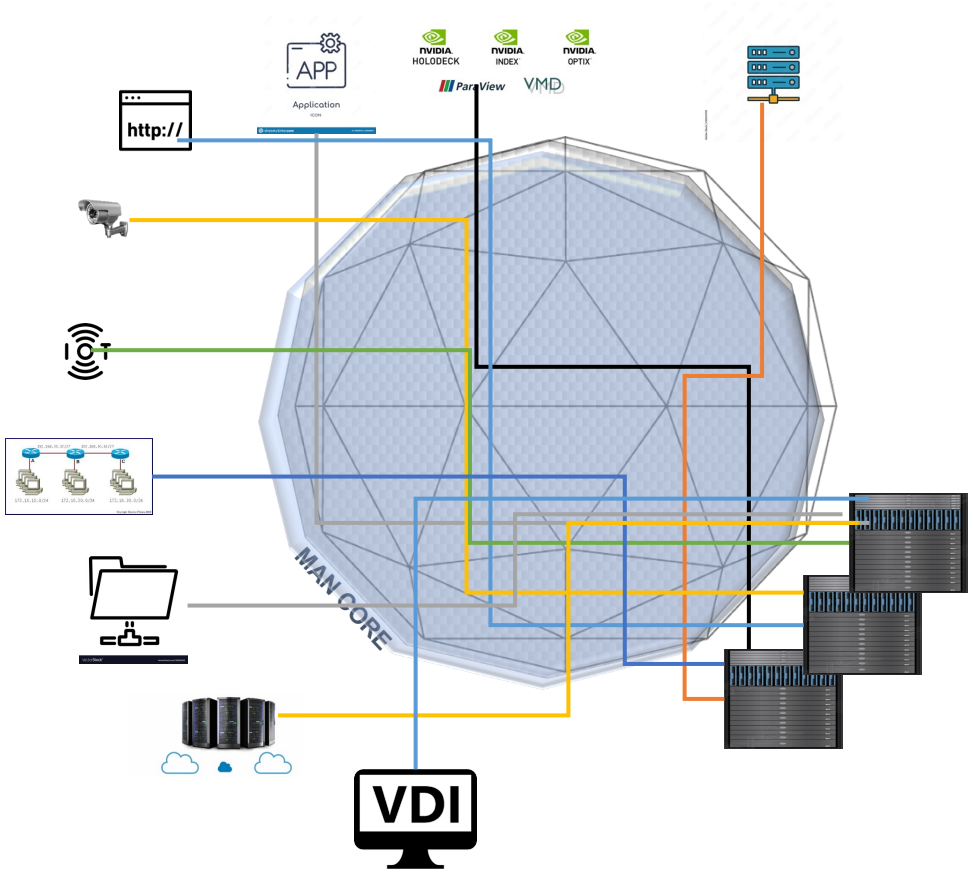




Per consentire il massimo grado di automazione, la rete deve mantenersi semplice e robusta

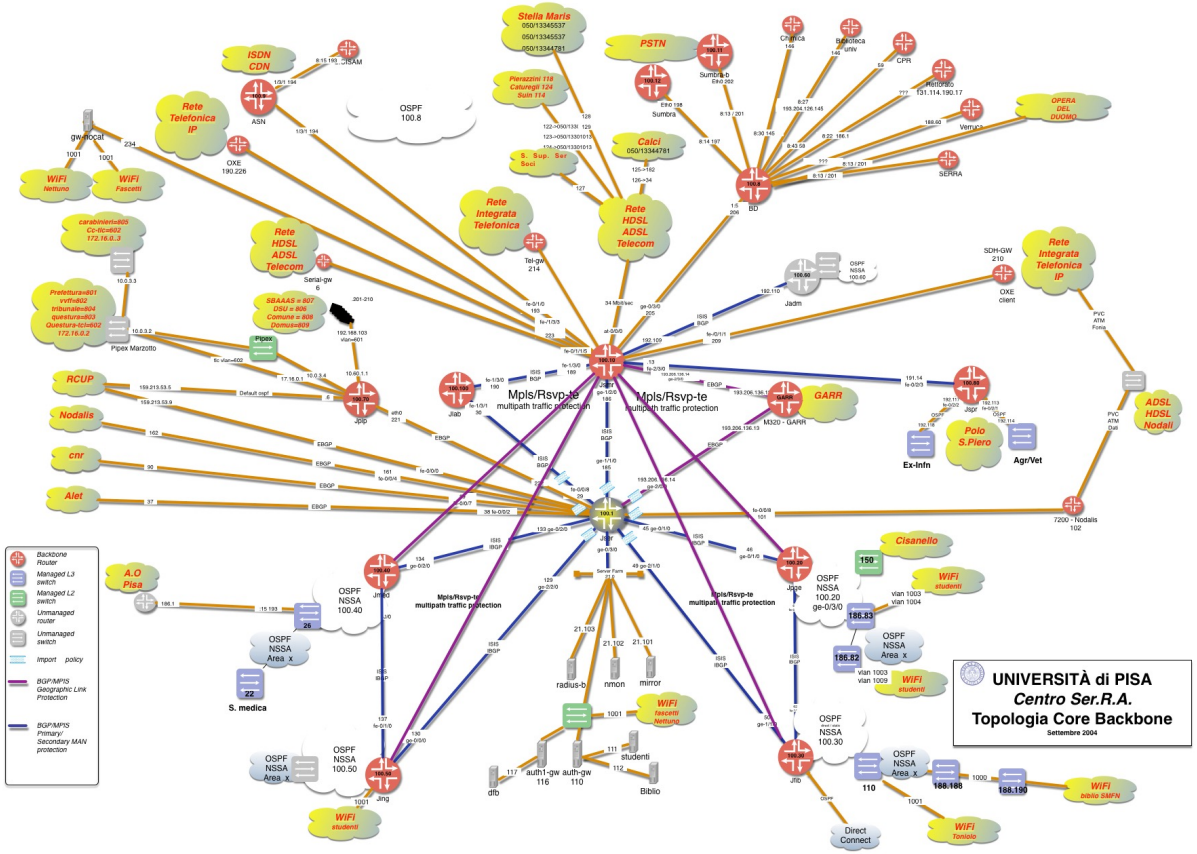
Disponibilità delocalizzata delle risorse

Esempi di risorse	
URL	VDI
Host	Application
IoT	SAML SP
Subnet	HPC farm
Windows Domain	Web
Server Farm	Network Share



Obiettivo: separazione fra infrastruttura fisica e servizi offerti

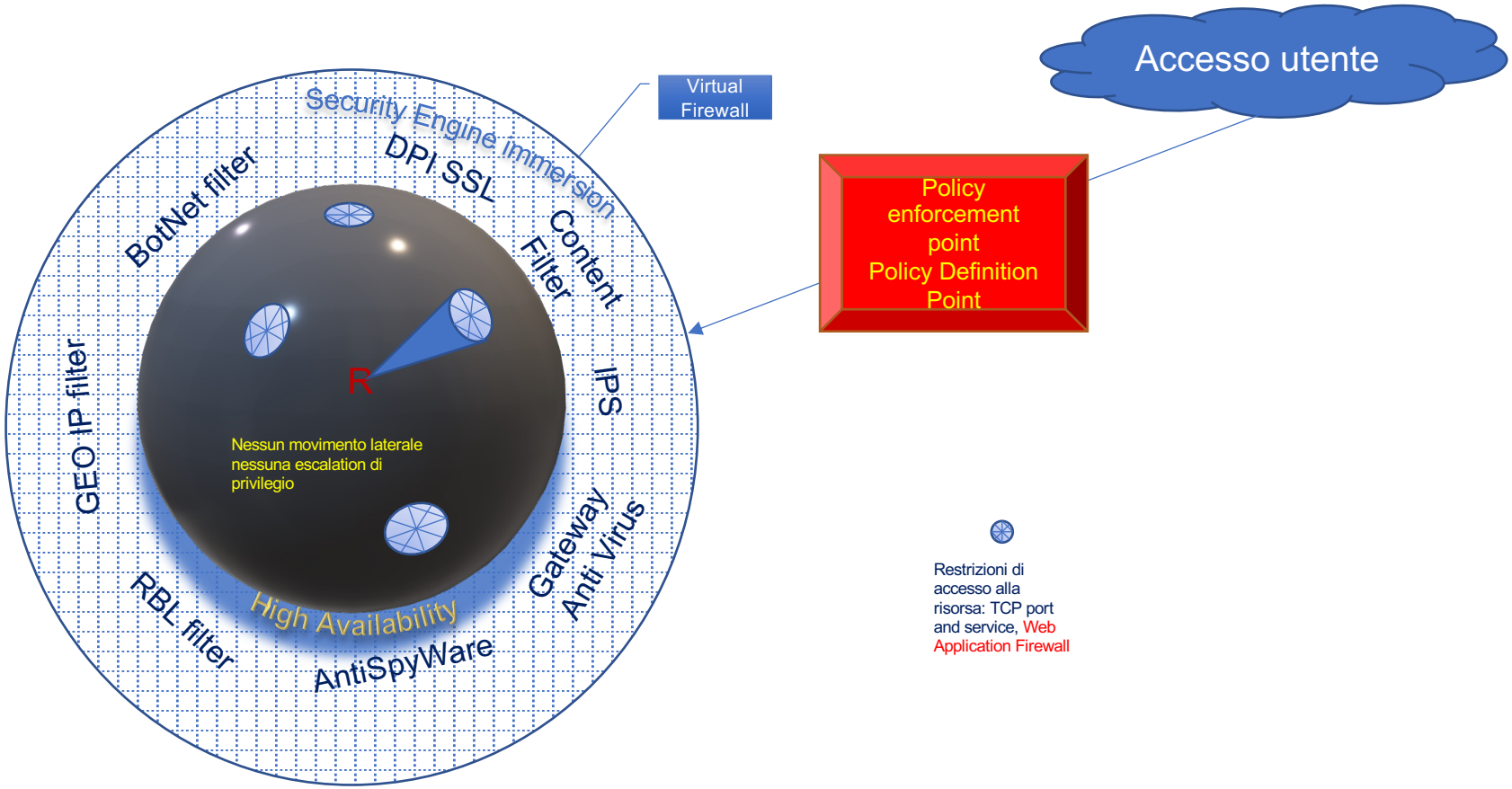
Da dove veniamo … rete basata su servizi L3. MPLS/RSVP/te transport per il supporto alla multitenancy e overlay network



Ottenere lo stesso obiettivo di una delocalizzazione semplice delle risorse (da un punto di vista provisioning e fruibilità), in questo contesto, è un compito assai più arduo

Protezione delle risorse cloud/backbone: modello Bubble Security

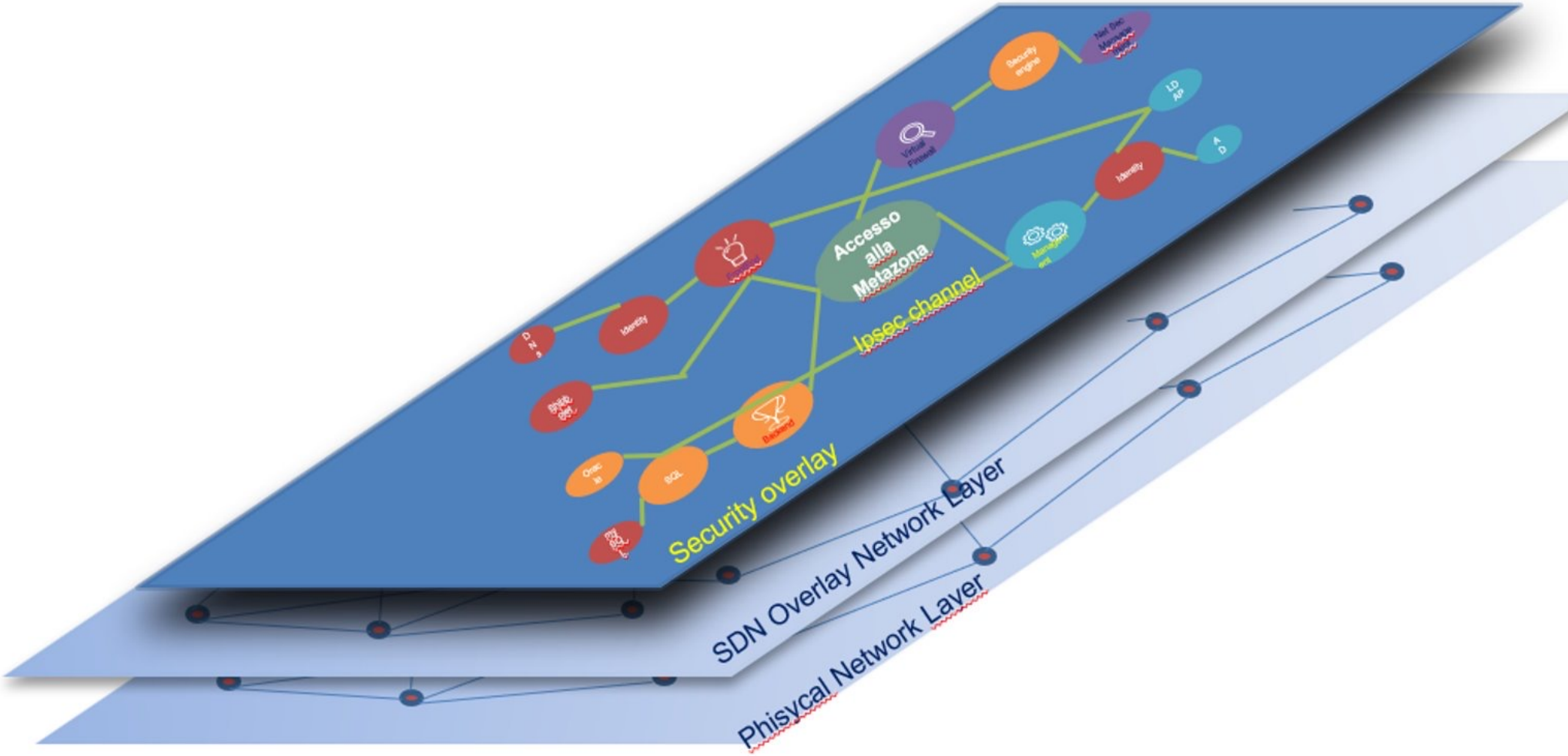
(linee guida ZTA: ognu tente o spostamento fra risorse deve essere escplicitamente autorizzato)



Ogni bolla caratterizzata da un fattore di opacità, cardinalità delle risorse, distribuzione geografica

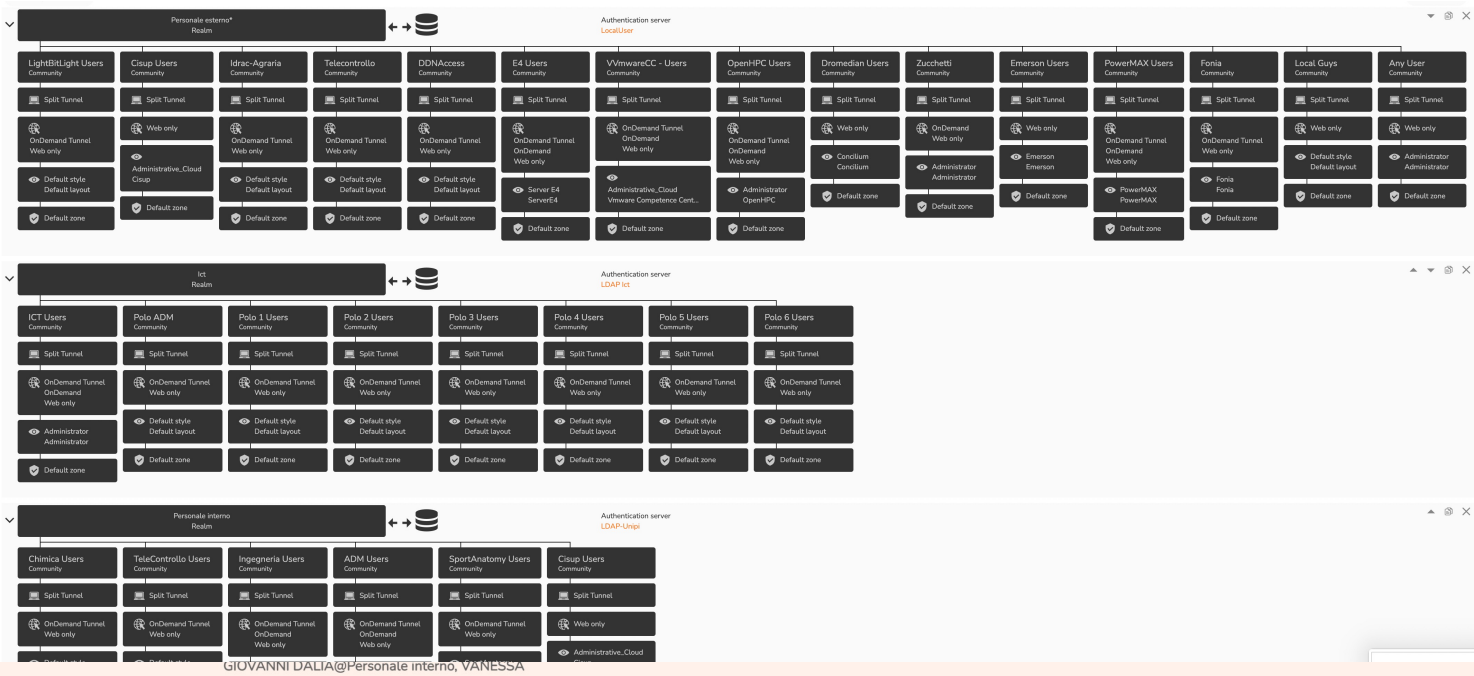
Bubble security , consentire l'accesso alle risorse senza complicare la rete con il routing: gli spostamenti fra le bolle: la Metazona

Comunicazione fra reti protette senza la complessità del routing
Garantisce sicurezza e integrità del movimento
Possibilità di disegnare ogni topologia di rete desiderata, svincolata dall'architettura fisica



Bubble Security, il controllo dell’accesso degli utenti alle risorse:
VPN SMA (Sonicwall Mobile Access) –applicazione dei principi ZTA no trust, no defense perimeter, no DMZ…..

Combattere i ransomware: ACCESSI controllati del singolo utente (o gruppo), basati sul minimo privilegio che impedisca azioni (o spostamenti) non esplicitamente autorizzati



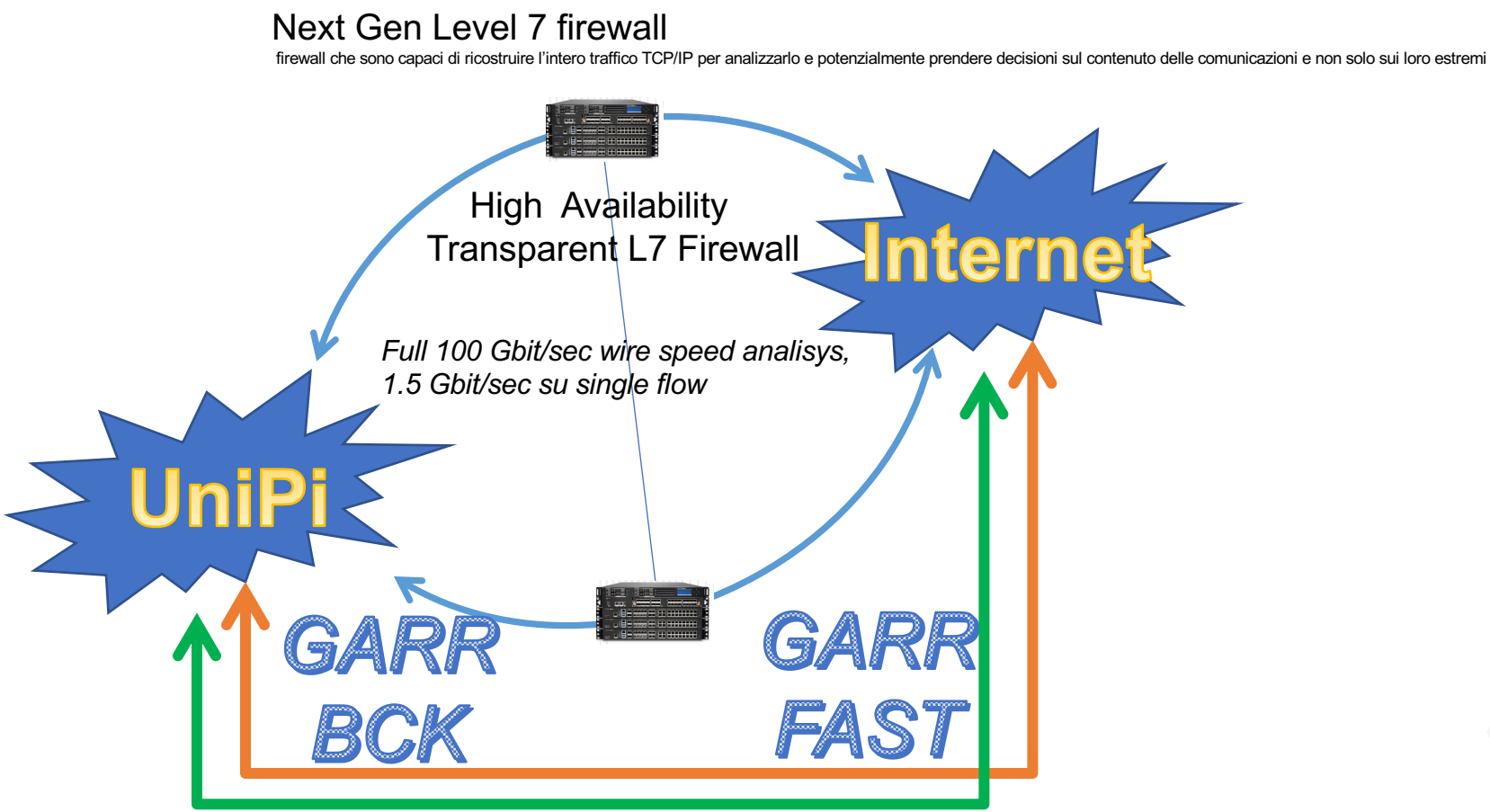
7	✓	Accesso Domotica Sapienza	GIOVANNI DALIA@Personale interno, VANESSA VASQUEZ@Personale interno, PATRIZIA MARCAURELIO@Personale interno, JONATHAN ADRAGNA@Personale interno	ServiziSicurezzaSapienza-Domotica	Any device zone	—

Applies to: Device zones
From: GIOVANNI DALIA@Personale interno , VANESSA VASQUEZ@Personale interno , PATRIZIA MARCAURELIO@Personale interno , JONATHAN ADRAGNA@Personale interno
To: ServiziSicurezzaSapienza-Domotica
Device zones: Any
Advanced: Permissi 10.114.189.103

8	✓	Accesso ABTelematica Antiincendio Sapienza	alupi	ServiziSicurezzaSapienza-antiincendio	Any device zone	—

Applies to: Device zones
From: alupi
To: ServiziSicurezzaSapienza-antiincendio
Device zones: Any
Advanced: Permissions: Read

L’accesso a Internet



Bubble Security, L’analisi perimetrale storica: Analitycs Report – fondamentale in caso di attacco ransomware, ricostruzione perimetri di attacco e c2c

Applications | Users | IP Addresses | Virus | Intrusions | Spyware | Locations | Botnets | Web Categories

Search... | IPv4 & IPv6 | View: Since Restart

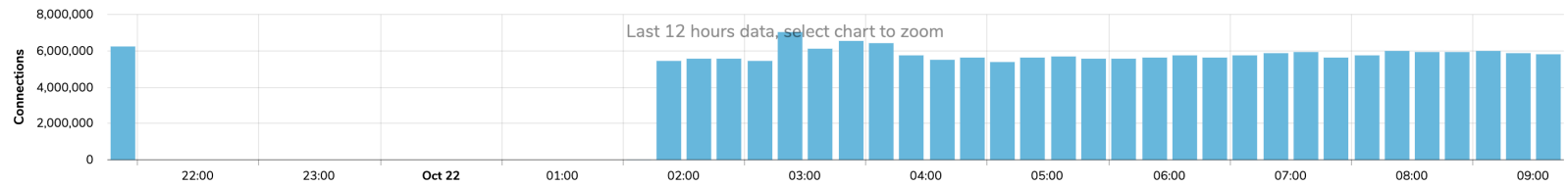
#	APPLICATION NAME	SESSIONS COUNT	SESSIONS PERCENTAGE
1	Service RPC Services	1.35B	179
2	Service RPC Services (IANA)	1.01B	139
3	General HTTPS	683.30M	99
4	General UDP	530.49M	79
5	General TCP	422.85M	59
6	General HTTP	363.61M	49
7	Service iMesh	340.85M	49
8	SSL/TLS--Version TLSv1.2-7927	312.00M	49
9	General DNS	220.85M	29
10	DNS Protocol--Standard Query .net Network Domains-6820	217.56M	29
11	Service Echo	206.48M	29
12	General Telnet	195.96M	29
13	General SSH	180.08M	29
14	Service Tivo TCP Data	139.48M	19
15	DNS Protocol--Standard Query .com Commercial Domains-6818	122.02M	19
16	General SIP control	102.85M	19
17	General SNMP	95.29M	19
18	Service SMB	83.97M	19
19	Encrypted Key Exchange--TCP Random Encryption(Skype,UltraSurf,E-5	74.64M	09
20	Service MS SQL	67.99M	09
21	Service NTP	65.17M	09

Session logs

/ Tenant - LocalDomain / SW-Frontier

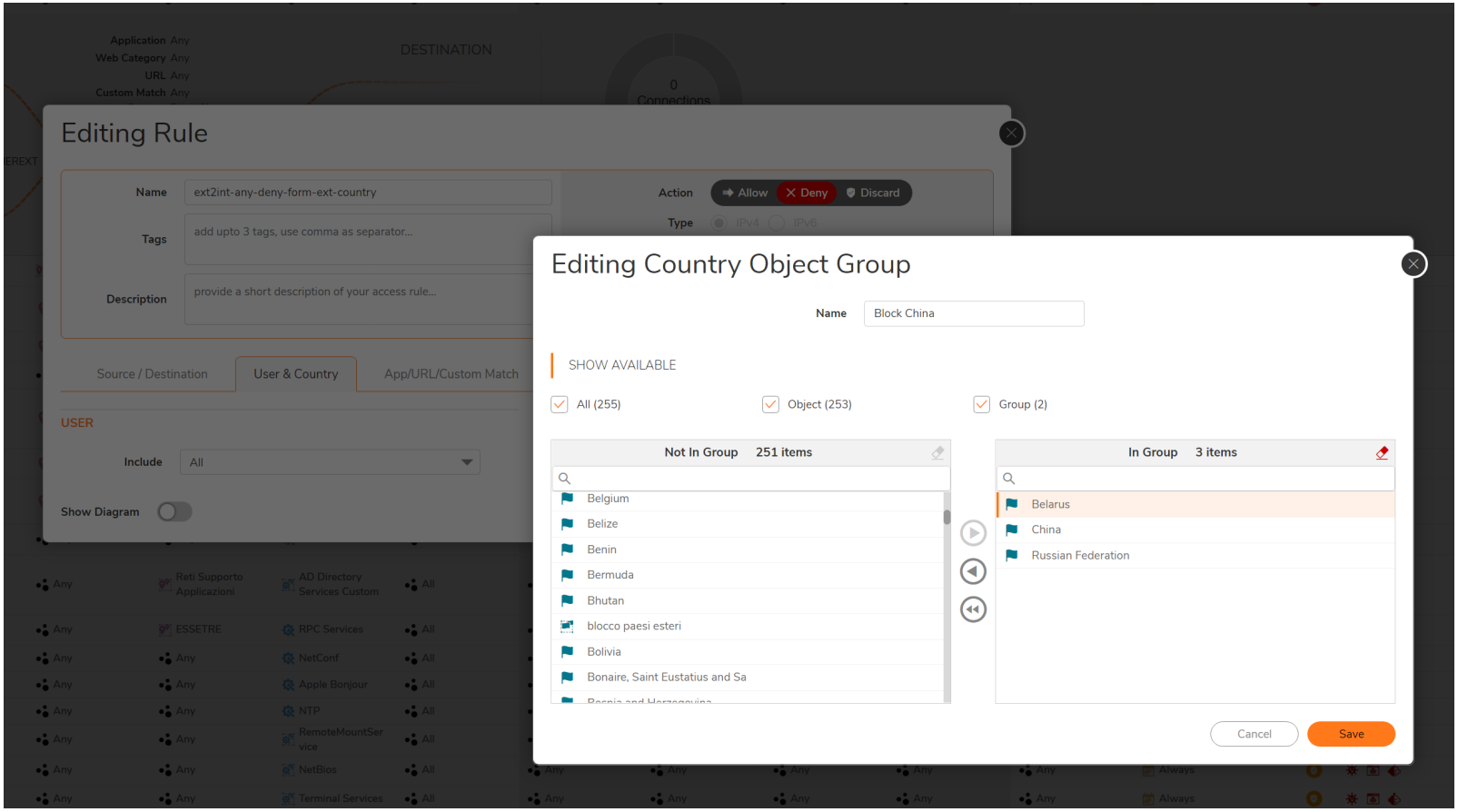
5 mins | Custom | 2022-10-22 03:45 To 2022-10-22 09:45 | Limit: 50

Applications : General TCP



#	OPEN TIME	ACTION	APPLICATION	APP CATEGORY	APP RISK	SIGNATURE	INIT IP	RESP IP	INIT	CONTRO...
1	09:45:06 Oct 22	Allowed	General TCP	Networking	Low	General TCP -- 49...	87.246.7.48	131.114.2.32		
2	09:45:06 Oct 22	Allowed	General TCP	Networking	Low	General TCP -- 49...	87.246.7.198	131.114.225.100		
3	09:45:06 Oct 22	Allowed	General TCP	Networking	Low	General TCP -- 49...	45.227.253.99	131.114.54.75		
4	09:45:06 Oct 22	Allowed	General TCP	Networking	Low	General TCP -- 49...	87.246.7.198	131.114.200.63		
5	09:45:06 Oct 22	Allowed	General TCP	Networking	Low	General TCP -- 49...	45.93.16.71	131.114.129.239		
6	09:45:06 Oct 22	Allowed	General TCP	Networking	Low	General TCP -- 49...	45.227.253.99	131.114.54.75		
7	09:45:06 Oct 22	Allowed	General TCP	Networking	Low	General TCP -- 49...	139.162.190.203	131.114.2.87		
8	09:45:06 Oct 22	Allowed	General TCP	Networking	Low	General TCP -- 49...	87.246.7.57	131.114.201.79		
9	09:45:06 Oct 22	Allowed	General TCP	Networking	Low	General TCP -- 49...	192.241.217.98	131.114.225.183		
10	09:45:06 Oct 22	Allowed	General TCP	Networking	Low	General TCP -- 49...	45.227.253.99	131.114.51.49		
11	09:45:06 Oct 22	Allowed	General TCP	Networking	Low	General TCP -- 49...	45.93.16.71	131.114.224.23		
12	09:45:06 Oct 22	Allowed	General TCP	Networking	Low	General TCP -- 49...	139.162.190.203	131.114.203.240		

Politiche georeferenziabili



Bubble Security, un accesso «particolare»: il servizio di posta elettronica: analisi degli allegati e controllo del phishing Capture Security Appliance / URL rewriting/User sendbox

ALL FILES	PENDING	RUNNING	FAILED	BENIGN	MALICIOUS	ALLOW / BLOCK LIST
1,020,74	0	0	0	1,019,43	1,309	0

Filter submitters... | Filter | Search (i.e. file name, etc.) | All | Custom | Column Selection | Export | Refresh

VERDICT | Malicious ×

#	VERDICT	FILE NAME	URL	FRIENDLY NAME	FROM	TYPE	DATE TIME	SOURCE	DESTINATION
1	Malicious	Medwin Publishers....		SW-FRONTIER	2CB8ED8231C0	Composite Document File V2 Document	Feb 23, 2022 - 22:28	1.9.83.51:32796	131.114.142.148:25
2	Malicious	xlXLiveScenes.zip?v...	s1.biz.xunlei.com/xlXLiveScenes.zip?v=1570789681	SW-FRONTIER	2CB8ED8231C0	Zip archive data	Jan 28, 2022 - 10:44	101.226.26.207:80	131.114.208.190:49476
3	Malicious	AllUserScene.zip?v=...	s1.biz.xunlei.com/AllUserScene.zip?v=1565580165	SW-FRONTIER	2CB8ED8231C0	Zip archive data	Jan 28, 2022 - 10:44	101.226.26.207:80	131.114.208.190:49487
4	Malicious	VipRenewalScene.zi...	s1.biz.xunlei.com/VipRenewalScene.zip?v=1545371773	SW-FRONTIER	2CB8ED8231C0	Zip archive data	Jan 28, 2022 - 10:44	101.226.26.207:80	131.114.208.190:49466
5	Malicious	LeaveBigRWebGam...	s1.biz.xunlei.com/LeaveBigRWebGameUserScene.zip?v=1...	SW-FRONTIER	2CB8ED8231C0	Zip archive data	Jan 28, 2022 - 10:44	101.226.26.207:80	131.114.208.190:49452
6	Malicious	ActiveBigRWebGa...	s1.biz.xunlei.com/ActiveBigRWebGameUserScene.zip?v=1...	SW-FRONTIER	2CB8ED8231C0	Zip archive data	Jan 28, 2022 - 10:44	101.226.26.207:80	131.114.208.190:49451
7	Malicious	LeaveBigRWebGam...	s1.biz.xunlei.com/LeaveBigRWebGameUserScene.zip?v=1...	SW-FRONTIER	2CB8ED8231C0	Zip archive data	Jan 28, 2022 - 09:55	101.226.27.225:80	131.114.208.190:44096
8	Malicious	xlXLiveScenes.zip?v...	s1.biz.xunlei.com/xlXLiveScenes.zip?v=1570789681	SW-FRONTIER	2CB8ED8231C0	Zip archive data	Jan 28, 2022 - 09:54	101.226.27.225:80	131.114.208.190:1059
9	Malicious	ActiveBigRWebGa...	s1.biz.xunlei.com/ActiveBigRWebGameUserScene.zip?v=1...	SW-FRONTIER	2CB8ED8231C0	Zip archive data	Jan 28, 2022 - 09:55	101.226.27.225:80	131.114.208.190:50084
10	Malicious	WebGameUserScen...	s1.biz.xunlei.com/WebGameUserScene.zip?v=1571109786	SW-FRONTIER	2CB8ED8231C0	Zip archive data	Jan 28, 2022 - 09:55	101.226.27.225:80	131.114.208.190:1077
11	Malicious	ActiveBigRWebGa...	s1.biz.xunlei.com/ActiveBigRWebGameUserScene.zip?v=1...	SW-FRONTIER	2CB8ED8231C0	Zip archive data	Jan 28, 2022 - 09:54	101.226.27.225:80	131.114.208.190:61518
12	Malicious	VipCashScene.zip?v...	s1.biz.xunlei.com/VipCashScene.zip?v=1573526235	SW-FRONTIER	2CB8ED8231C0	Zip archive data	Jan 28, 2022 - 10:46	101.226.27.225:80	131.114.208.190:58976
13	Malicious	VipCashScene.zip?v...	s1.biz.xunlei.com/VipCashScene.zip?v=1573526235	SW-FRONTIER	2CB8ED8231C0	Zip archive data	Jan 28, 2022 - 09:57	101.226.27.228:80	131.114.208.190:51102
125	Malicious	gameShieldDll.dll?h...	109.105.133.6/files/gameshield_64/360.17.9.31/gameShie...	SW-FRONTIER	2CB8ED8231C0	PE32+ executable (DLL) (console) x86-64	Jan 29, 2022 - 00:50	109.105.133.6:80	131.114.234.131:51871
126	Malicious	/info.zip		SW-FRONTIER	2CB8ED8231C0	Zip archive data	Jan 30, 2022 - 00:56	109.195.146.70:513	131.114.44.247:65535
1						archive data	Feb 18, 2022 - 23:11	109.195.147.173:34	131.114.142.148:25
1						archive data	Feb 18, 2022 - 00:03	109.195.147.173:40	131.114.142.148:25
1						archive data	Feb 18, 2022 - 17:22	109.195.147.173:42	131.114.142.148:25
1						archive data	Feb 18, 2022 - 01:48	109.195.147.173:47	131.114.142.148:25
1						2+ executable (GUI) x86-64	Feb 15, 2022 - 12:04	109.234.37.30:80	131.114.216.101:58865

SCARICA PDF

URL rewriting

https://es.sonicurlprotection-fra.com/click?PV=2&MSGID=202210201730310847806&URLID=3&ESV=10.0.18.7423&IV=D15D5FC240DCBFD5A383157B709F8268&TT=1666287031982&ESN=j0M%2BoYN3ckSU7AUVnc5mYumzxX1Zor%2FUQ0I4hpqQS3Y%3D&KV=1536961729280&B64_ENCODED_URL=aHR0cHM6Ly9hZG1pbnBvcnRhbC5hcHBhcm91bmQuY29tL2FwaS9jcHEvQ29uZmlndXJhdG9yL09mZmVyLz91cmxEYXRhPVJRY0lGbmJRSDc3dVJuYmZaWTB5VDdiNE9XOWFwVFpLYUh6eXp3YlIPYXorSk50NmdYdTRFWmd3YTNhdTY2WmRTQ2hob2owUU1ibWJ2dnM0Tk9MR0w4NTQ0Yi9jemZsZzJ3Q3k5bCt0Wm5XSXkxWXVldmswNncIM2QlM2QmcD1RVU5mTWpBd1h3PT0&HK=6347CB35A1D83B2B27C594DF98BB4D15B8B2F4DA3D2AFE94596EAD32A634659D

UNI EN ISO 9001:2015
UNI EN ISO/IEC 27001:2013
ISO 9001 ACSO Certification Body

Ogni ora Connessioni attendibili e bloccate

Spam rewriting

WORKSHOP GARR 2022 NET MAKERS

Reportistica: il controllo dei flussi

Capture Security Appliance

Report storica: Daily report Analityc

Analytics Unipi Frontier

Schedule Name:
Sonicwall Frontier

Report on Firewall:
SW-Frontier (2CB8ED8231C0)

Firewall Type:
SuperMassive

Report Period:
March 11, 2022 00:00:00 to March 11,

Table of Contents

Details - Applications .....
Details - Users .....
Details - Virus .....
Details - Botnet .....
Details - Initiator IPs .....
Details - Initiator Locations .....
Details - Responder IPs .....
Details - Responder Locations .....
Details - BW Queues .....
Details - Threats .....
Details - Blocked .....
Summary - Applications .....
Summary - Users .....
Summary - Virus .....
Summary - Initiator IPs 25
Summary - Responder IPs 27
Summary - Initiator Locations 29
Summary - Responder Locations 30
Summary - BW Queues 31
Summary - Threats 32
Summary - Blocked 33

Details - Applications

(Continued)

This section provides a detailed list of the applications that were active on your network during the reporting period. Furthermore, the top applications have been plotted on the charts below to give you insight into the traffic load, as well as any threats associated with those applications.

Name	Sessions	Data Transferred	Total Threats	Total Blocked
Windows Update	1.54×10^6	1.47 TB	0	0
HTTP Protocol	3.79×10^6	1.10 TB	193	1
Microsoft SharePoint	1.03×10^6	948.66 GB	0	0
RTP	4.45 K	885.09 GB	0	0

Data View by Total blocked

Name	Sessions	Data Transferred	Total Threats	Total Blocked
Service SMB	3.86×10^6	203.51 MB	0	3.69×10^6
Service Terminal Services TCP	2.76×10^6	598.61 MB	0	2.61×10^6
General SNMP	2.24×10^6	456.29 MB	0	1.92×10^6
Service NTP	2.76×10^6	346.66 MB	0	1.48×10^6
Service NetBios SSN TCP	749.61 K	36.75 MB	0	741.09 K
General NETBIOS	696.28 K	54.10 MB	0	684.26 K
Service Apple Bonjour	541.18 K	42.15 MB	0	541.15 K
Service RPC Services	48.73×10^6	56.35 GB	78	536.66 K
General TCP	134.23×10^6	94.88 GB	0	482.91 K
Service RPC Services (IANA)	19.46×10^6	3.96 GB	0	269.30 K

Reportistica storica: Daily report CSA

Capture Appliance Scheduled Report

FileCaptureReport - CSA1000

Mar 11 2022 22:59:02 GMT
Report Period: 1 Day(s)
Serial Number: 2CB8ED826E33
WAN IP: 10.10.10.50

FileCaptureReport - CSA1000
Mar 10 2022 22:59:00 GMT to Mar 11 2022 22:59:00 GMT

Usage Summary

Total files submitted	23854	↑
Total malicious files found	24	↑
Total number of unique submitters	2017	↓

Verdict Breakdown by Stage

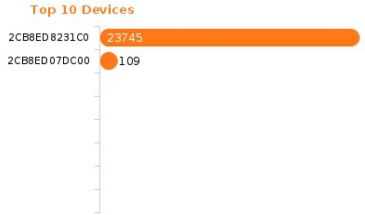
Analysis Stages	Malicious	Clean
Static Analysis		8734
Reputation	10	4871
Dynamic Analysis	14	10225
Allowlist/Blocklist		

Processing Time Statistics (seconds)

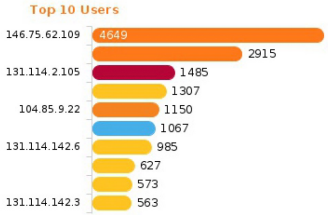
	Average	Median	Min	Max
Analysis Time	39	10	0	1000
Queue Time	0	0	0	43

FileCaptureReport - CSA1000
Mar 10 2022 22:59:00 GMT to Mar 11 2022 22:59:00 GMT

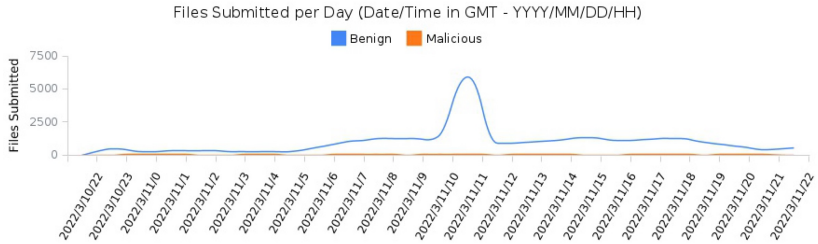
Top 10 Devices Submitting Files



Top 10 Users Submitt



Files submitted per day



Accesso degli utenti «standard» alla rete: la campus network

- Campus network, spesso l'anello «debole» della catena, sicuramente nostra criticità

  Alta resilienza e fast convergence ? Se ne può fare a meno.. Spesso SPT e nessun controllo delle porte

  Gli accessi agli armadi di distribuzione sono spesso non protetti e la segregazione a livello trasporto non è sempre granulare

  Sufficiente Passive check monitoring – SNMP nessun telemetria e nessun controllo real time delle attività

  Aggiornamento, / archiving, versioning e gestione degli accessi quando necessario (ma se non è obbligatorio, alla fine, si fa?

Considerare le reti campus di serie B è un grossolano errore molto diffuso……perché..

…I problemi di sicurezza arrivano in grandissima parte da host della rete campus

- Le evidenze dell'attacco ransomware a UNIPI : da dove provengono i dati esfiltrati? Data Breach, quasi sempre all'edge.
- Inoltre:

La trasformazione digitale degli ultimi 3 anni ha incrementato enormemente il network workload e la necessità di garanzia di servizio in continuità end-to-end e di conseguenza la necessità di scalabilità ,programmabilità, dinamicità, sicurezza, analytic capabilities, e tool di management e provisioning.

Nelle reti Campus il numero dei dispositivi cresce significativamente -> anche le operazioni più banali diventano pesanti (es. cambio password di management., o configurazione di una vlan su 300 switch)

La soluzione è, per noi, work in progress…

- Fabric (Extreme Network Fabric Connect) anche per le reti legacy

(IEEE 802.1aq/ShortestPathBridge, control plane, IEEE 802.1h/Mac-in-Mac data plane)

- Telemetria – controllo (storico) delle attività di rete in modalità push

- Network (aaS) automation e auto provisioning/removing degli end point

gestione error-free e scalabilità: Generalmente lo stretching di una risorsa richiede la configurazione di molti nodi della rete: obiettivo configurazione dei servizi end to end solo sul perimetro

- Endpoint control – sicurezza dei sistemi al momento dell' accesso

- Piattaforma centralizzata di gestione (xIQ)

Controllo accessi nelle reti legacy (BYOD, IoT, Dispositivi etc.)

Prereq: Directory Service (Radius, LDAP, AD..etc)

802.1x (IoT, nessuna maggiore sicurezza all'edge)

NAC solution/captive portal

AD (SingleSignOn),

Tutte queste sono soluzioni non sono frictionless per gli utenti e sono di difficile gestione su una grande comunità, ma le soluzioni NAC consentono un controllo maggiormente granulare su utenti e IoT device:

- role based access control.
- troubleshooting
- pro-active performance monitoring