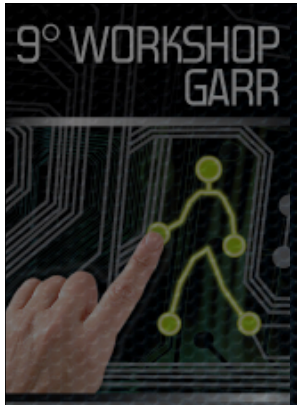


Al servizio degli utenti

quando tecnologie complesse incontrano la semplicità di utilizzo

Roma
15-18 GIU 09

La virtualizzazione delle risorse di rete e dei sistemi di sicurezza: l'implementazione di router e firewall virtuali sul bordo di una rete dati di accesso al GARR

Giuseppe MARULLO, Antonio CAMPA, Antonio TOMMASI, Marco FERRI

Ufficio Gestione Dorsale di Ateneo

dorsale@unisalento.it

I contesti in cui è necessario affrontare le problematiche di **firewalling**, **intrusion detection system** (**IDS**) ed **intrusion prevention system** (**IPS**) richiedono sistemi sempre più capaci di garantire:

- alte prestazioni;
- supporto dei protocolli di comunicazione;
- interoperabilità tra sistemi e servizi;
- affidabilità;
- contenimento dei consumi e dei costi;
- gestibilità, modularità, espandibilità e flessibilità.

Tutte le organizzazioni che si affacciano su Internet sono sempre più portate ad erogare grandi quantità di contenuti informativi ad un'utenza sempre più vasta traendo benefici da:

- una rete della ricerca sempre più fortemente interconnessa e veloce, oltre che a qualità garantita e controllata (si pensi al progetto **GARR-X**);
- lo sviluppo di servizi di ricerca aperti e diffusi come per esempio le **griglie computazionali**;
- l'evoluzione dei servizi di didattica e collaborativi (WEB 2.0, E-Learning 2.0) sempre più orientati al WEB e pertanto più fruibili dall'utenza.

D’altro canto, la diffusione e la disponibilità per studenti, docenti, ricercatori ed imprese, di accessi ad Internet sempre più veloci (in ogni posto, in mobilità ed in ogni momento) che spaziano dalla **connettività wired** (xDSL) alla **connettività wireless** (WiFi, WiMax ecc.), costringe le organizzazioni della ricerca e della didattica a dotarsi di servizi di connettività ad Internet sempre più ad **alta capacità**.

Con la prospettiva di dover continuamente potenziare i propri collegamenti ad Internet, le organizzazioni si trovano costrette ad effettuare **continui investimenti** per dotarsi di sistemi di **controllo passivo**, **attivo** o **proattivo** sul traffico da esse veicolato.

Tali sistemi di controllo del traffico operano a vari livelli:

- bordo della **Rete di Ateneo**;
- bordo della **Rete di Campus**, **Edificio** o di singola struttura (**laboratorio**, **dipartimento**, **facoltà**, etc.);
- protezione dei singoli **Server**.

Concentrando l'attenzione su di un apparato di sicurezza quale un **firewall di bordo di Ateneo**, questo deve essere potenzialmente dimensionato in maniera tale da garantire un throughput comparabile con la velocità di trasferimento dati che l'organizzazione possiede per l'accesso alla rete **GARR** e/o al suo **ISP**.

Il problema è che sempre più la velocità di accesso si avvicina al Gigabit per secondo, sempre più aumenta la necessità di dotarsi di firewall di bordo in grado di **garantire prestazioni elevate**.

Evidentemente, un tale apparato di rete dovrà essere collegato al **router di bordo** da un lato e dall'altro agli apparati **core** della rete.

Sicurezza al confine della rete di Ateneo

L'esperienza dell'**Università del SALENTO** ha portato ad individuare, nel corso del tempo, alcune caratteristiche fondamentali per un sistema di sicurezza al bordo della rete di Ateneo:

- analisi minima del flusso di dati;
- impiego di access list "leggere";
- NAT e PAT per le reti private di Ateneo;
- logging storico e puntuale del traffico.

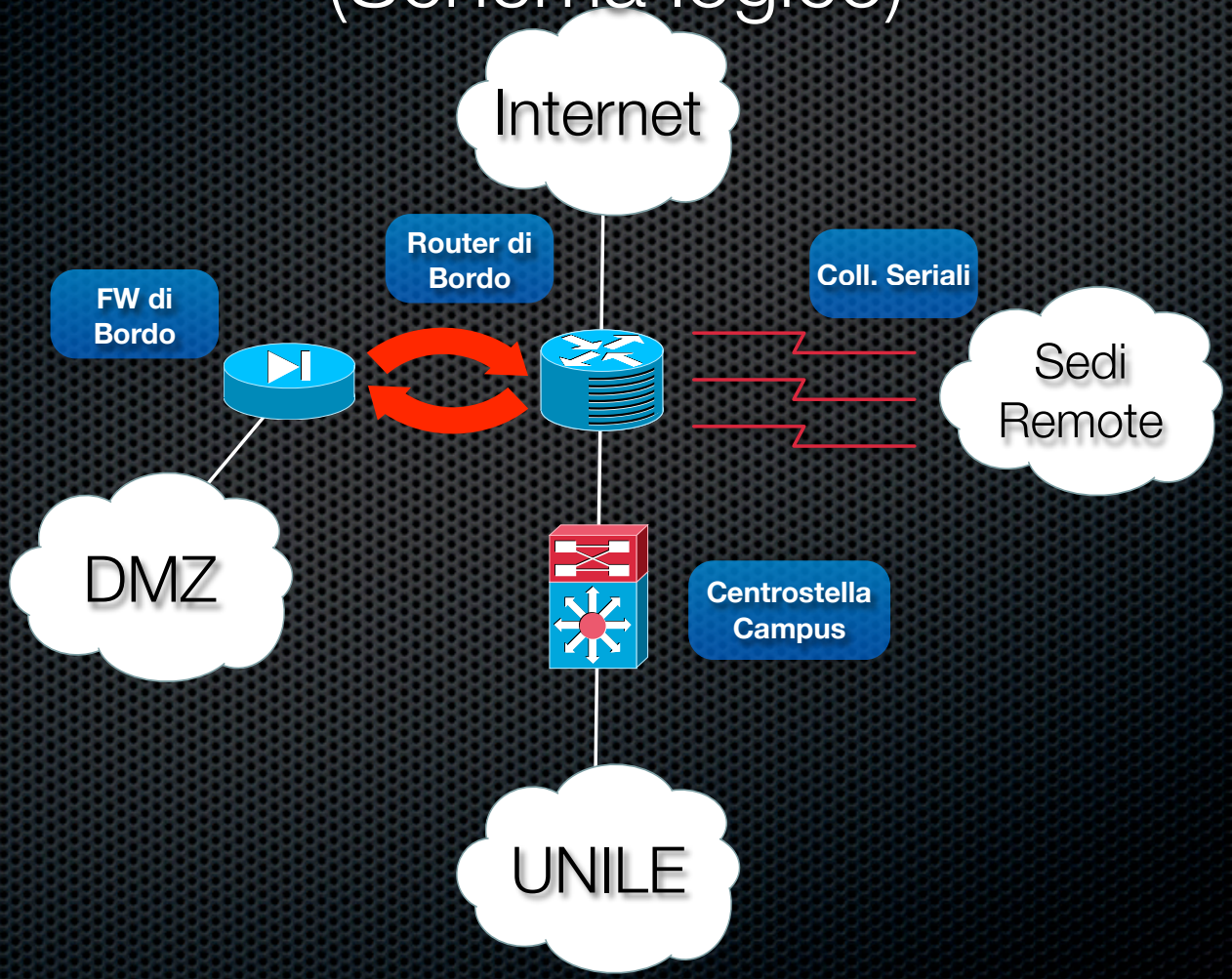
Contesto di partenza

L'Università del Salento, nell'ottica dell'espansione della propria architettura di rete **LAN/WAN** e di creazione di una propria **MAN** in fibra ottica, ha avviato nel 2008 un progetto di integrazione di nuove tecnologie di connettività, e contemporaneamente di ristrutturazione, volto a sostituire l'obsoleto Cisco 7507 (facente funzione di router di bordo) non più in grado di assicurare prestazioni allineate agli SLA richiesti con i nuovi e futuri scenari.

Contesto di partenza

- CISCO 7507 come **Router di Bordo**;
- CISCO PIX 525 come **Firewall di Bordo** e per la gestione della **DMZ**;
- **UpLink verso il GARR** tramite un collegamento **POS** a **155Mbit/s**;
- raccolta dei collegamenti seriali alle sedi universitarie (e non solo) sparse per il **Salento**;
- uso e abuso delle **Routing Map**.

Contesto di partenza
(Schema logico)



Contesto di arrivo

Per il nuovo apparato che si dovrà occupare di ottimizzare il **segmento perimetrale** della rete di Ateneo, si è pensato di scegliere un unico sistema modulare:

- che consentisse di rispettare gli attuali (e prossimi) SLA;
- che includesse un più performante sistema di firewalling;
- che permettesse la ridondanza dei moduli e la gestione di router e firewall virtuali integrabili con la futura MAN MPLS;
- che riutilizzasse, in parte, gli investimenti fatti per il vecchio router (moduli e interfacce).

Contesto di arrivo

Dopo un'attenta valutazione costi/prestazioni, la scelta è caduta su di un CISCO 7609S con i seguenti moduli:

- Route Switch Processor 720 capace di un throughput di 400 Mpps e 720 Gbps;
- Firewall Module che arriva a gestire sino a 5.4 Gbps di traffico complessivo;
- Cisco Enhanced FlexWAN con una interfaccia POS e una ATM.

Contesto di arrivo

L'arrivo della **MAN in fibra** ha permesso di eliminare gran parte dei **collegamenti seriali** (siamo passati **da 15 a 3**) e questo ha permesso di utilizzare un piccolo router per la raccolta dei CDN, inserito, poi, all'interno della rete del Campus Universitario.

L'utilizzo di una **POS** per il **collegamento al GARR** ci ha spinto ad adottare fin da subito dei **contesti virtuali** di routing per il corretto inserimento del **FWSM** in quanto tale scheda/interfaccia non consente l'utilizzo del **tagging L2** normalmente utilizzato nella gestione del modulo di firewalling.

Contesto di arrivo
(Le VRF)

Attraverso il meccanismo di **Virtual Routing and Forwarding** (**VRF**) è possibile dividere un router o uno switch Layer 3 in diversi dispositivi virtuali indipendenti.

Le VRF portano a livello 3 le prerogative che le VLAN permettono di gestire a livello 2 e, in pratica, ogni router virtuale supporta una **singola tabella di routing virtuale**.

I router virtuali supportano i protocolli standard di routing, quali, ad esempio, l'**OSPF** o il **BGP**.

Il funzionamento di un protocollo di routing su di un router virtuale è indipendente dalle operazioni di routing sugli altri router virtuali nello stesso dispositivo fisico.

Contesto di arrivo
(Le VRF)

Possiamo gestire più VPN anche con overlapping degli indirizzi IP in quanto appartenenti a schemi logici isolati tra di loro.

Le funzioni NAT e di firewall nei router dotati di VRF funzionano (quasi sempre) all'interno di un router virtuale.

Ogni rete virtuale può avere, quindi, proprie policy di firewall e mantenere uno spazio separato di indirizzi IP.

L'unica maniera per poter far parlare VRF differenti di un unico router è quello di utilizzare **BGP** e le "**extended communities**" o, come nel nostro caso, un "apparato" esterno.

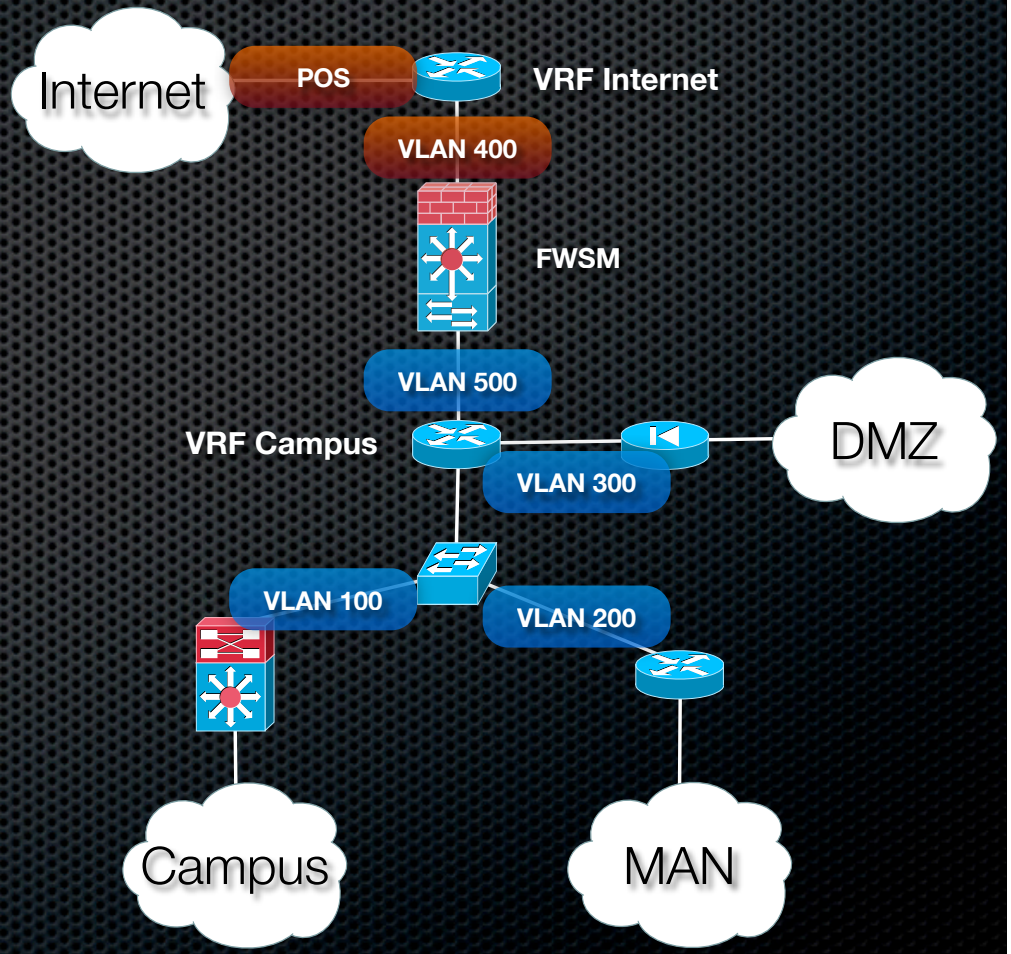
Contesto di arrivo
(Schema logico)

VRF Campus

```
vlan 100
 name To_Campus
vlan 200
 name To_MAN
vlan 300
 name To_DMZ
vlan 500
 name External1
```

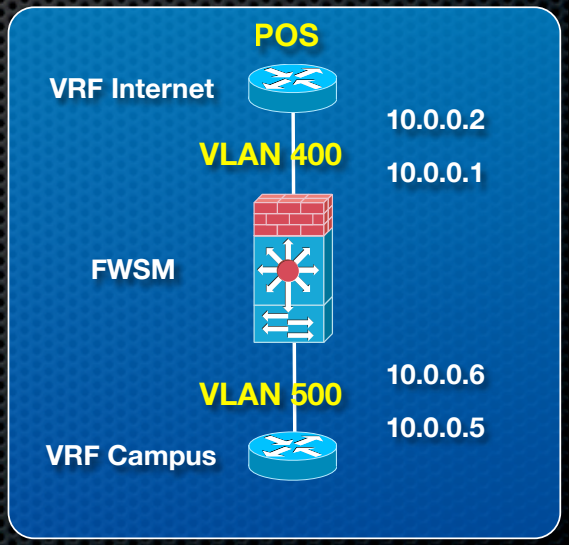
VRF Internet

```
interface POS2/0/0
vlan 400
 name External0
```



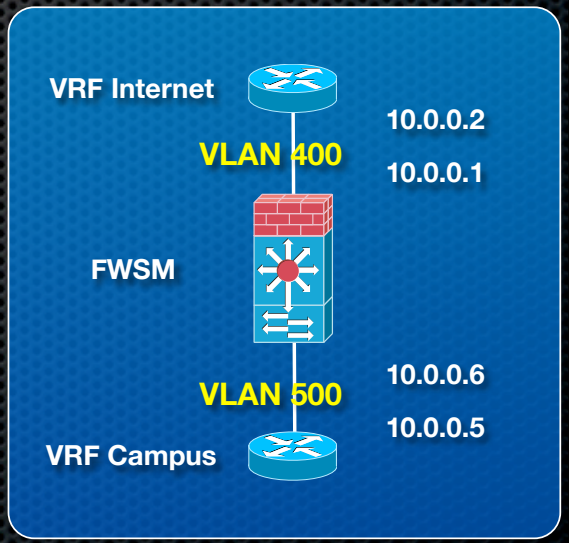
Contesto di arrivo
(Configurazione Router)

```
interface Vlan400
 ip vrf forwarding Internet
 ip address 10.0.0.2 255.255.255.252

interface Vlan500
 ip vrf forwarding Campus
 ip address 10.0.0.5 255.255.255.252

interface POS2/0/0
 ip vrf forwarding Internet
 ip address 193.206.137.x 255.255.255.252

ip route vrf Internet 0.0.0.0 0.0.0.0 193.206.137.y
ip route vrf Internet 193.204.w.0 255.255.240.0 10.0.0.1
ip route vrf Internet 212.189.z.0 255.255.240.0 10.0.0.1

ip route vrf Campus 0.0.0.0 0.0.0.0 10.0.0.6
```



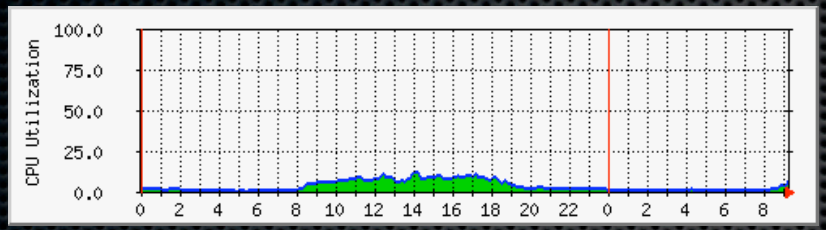
Contesto di arrivo
(Configurazione Firewall)

```
interface Vlan500
 nameif inside
 security-level 100
 ip address 10.0.0.6 255.255.255.252

interface Vlan400
 nameif outside
 security-level 0
 ip address 10.0.0.1 255.255.255.252


route outside 0.0.0.0 0.0.0.0 10.0.0.2 1

route inside 193.204.w.0 255.255.240.0 10.0.0.5 1
route inside 212.189.z.0 255.255.240.0 10.0.0.5 1
route inside 10.0.0.0 255.255.128.0 10.0.0.5 1
```

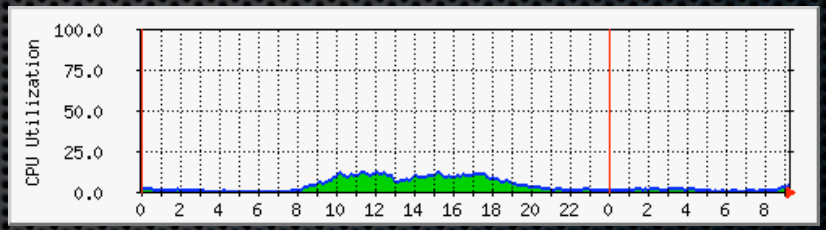


Contesto di arrivo
(Rilevazioni di utilizzo e considerazioni)

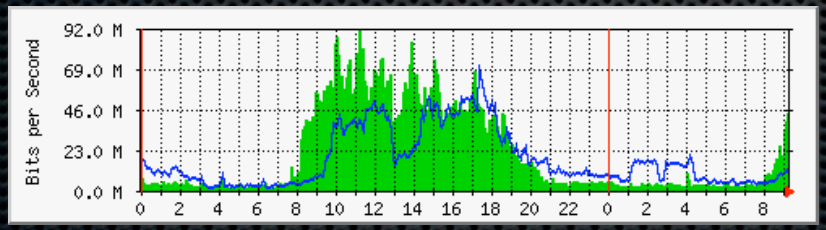
Utilizzo CPU Router (%)



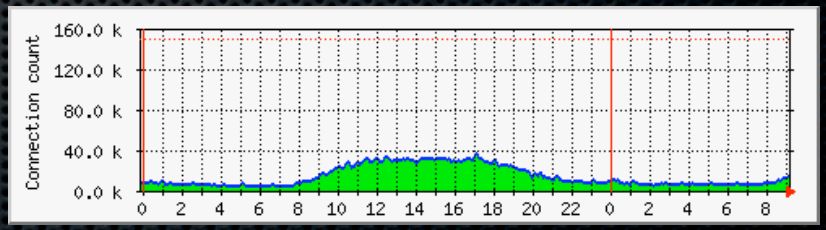
Utilizzo CPU FWSM (%)



Banda I/O (Mb/s)



Numero di connessioni



Contesto di arrivo
(Analisi puntuale e storica del traffico)

La posizione del firewall al bordo della rete di Ateneo permette di effettuare delle rilevazioni statistiche sul traffico in transito per l'intera struttura.

Le statistiche sullo **storico** si basano sull'analisi dei log inviati dal firewall ad un **syslog** esterno che, a seconda del grado di "**verbose**" impostato, possono scendere sino alla rilevazione della singola connessione (con conseguente impatto sul processore del modulo).

La rilevazione "**puntuale**" si basa sull'interrogazione del firewall circa le connessioni in transito in un determinato istante.

Contesto di arrivo
(Analisi puntuale e storica del traffico)

Terminal — ttyp1

```
Gimaru-MacBook-Pro:~ gimaru$ analisi_complessive.sh complessive_20090520120501

Data del check: 20/05/2009 12:05:01
Totale connessioni: 34660
Singoli host: 2084

Top 10 connessioni complessive:                          | Top 10 traffico TCP:
IP              connTCP  connUDP  connTOT  trTCP         | IP              connTCP  connUDP  connTOT  trTCP
193.204.xx.yy   575      3469     4044     1.1(GB)       | 212.189.xx.yy   62       0        62       2.3(GB)
193.204.xx.yy   863      3169     4032     93.5(MB)      | 193.204.xx.yy   68       562      630      2.3(GB)
193.204.xx.yy   2437     120      2557     478.2(MB)     | 10.0.72.yy      16       274      290      1.1(GB)
193.204.xx.yy   336      2214     2550     784.7(MB)     | 193.204.xx.yy   575      3469     4044     1.1(GB)
193.204.xx.yy   1375     0        1375     138.2(KB)     | 212.189.xx.yy   3        0        3        1.1(GB)
193.204.xx.yy   1135     0        1135     10.8(MB)      | 193.204.xx.yy   25       0        25       886.5(MB)
10.0.30.yy      155      856      1011     495.9(MB)     | 193.204.xx.yy   336      2214     2550     784.7(MB)
193.204.xx.yy   933      1        934      61.6(KB)      | 10.0.38.yy      4        2        6        584.6(MB)
193.204.xx.yy   127      607      734      35.5(MB)      | 212.189.xx.yy   5        0        5        560.1(MB)
193.204.xx.yy   649      21       670      121.1(MB)     | 10.0.30.yy      155      856      1011     495.9(MB)



Gimaru-MacBook-Pro:~ gimaru$
```

Contesto di arrivo
(Analisi puntuale e storica del traffico)

Il firewall si trasforma in un potente strumento di debug da utilizzare quando ci sono problemi sulla rete.

Per ogni singolo IP appartenente alle reti di Ateneo è possibile rilevare, ad esempio:

- elenco delle connessioni TCP attive (IN/OUT);
- elenco delle “pseudo-connessioni” UDP (IN/OUT);
- elenco degli host esterni che sono in relazione con l’IP considerato;
- traffico generato (TCP e/o UDP).

Particolarità emerse nell'uso delle VRF

Le VRF sono state utilizzate anche durante la migrazione di una sede remota (Cittadella della Ricerca - Brindisi) da un collegamento seriale ad un UpLink a 10Mb/s con un nuovo set di indirizzi IP pubblici direttamente con il GARR.

In questo caso le VRF hanno permesso di far convivere i vecchi IP con i nuovi sino alla migrazione completa e la relativa dismissione del CDN a 2 Mb/s.

In questa occasione sono state rilevate alcune anomalie nelle impostazioni e l'utilizzo del DHCP nel contesto dei router virtuali.

Particolarità emerse nell'uso delle VRF

Alcune tipologie di router (il router di bordo preso in considerazione è uno di questi) non permettono di utilizzare il NAT sulle interfacce associate alle VRF.

Quando si utilizzano le VRF insieme al BGP bisogna sempre ricordarsi che il processo di routing è solo uno e pertanto potrebbero presentarsi delle difficoltà nel caso in cui si vogliano gestire più **AS** su di un singolo router (reale).

In tale evenienza si può ricorrere all'utilizzo degli **AS privati** facendo particolare attenzione al **PATH** che viene annunciato.

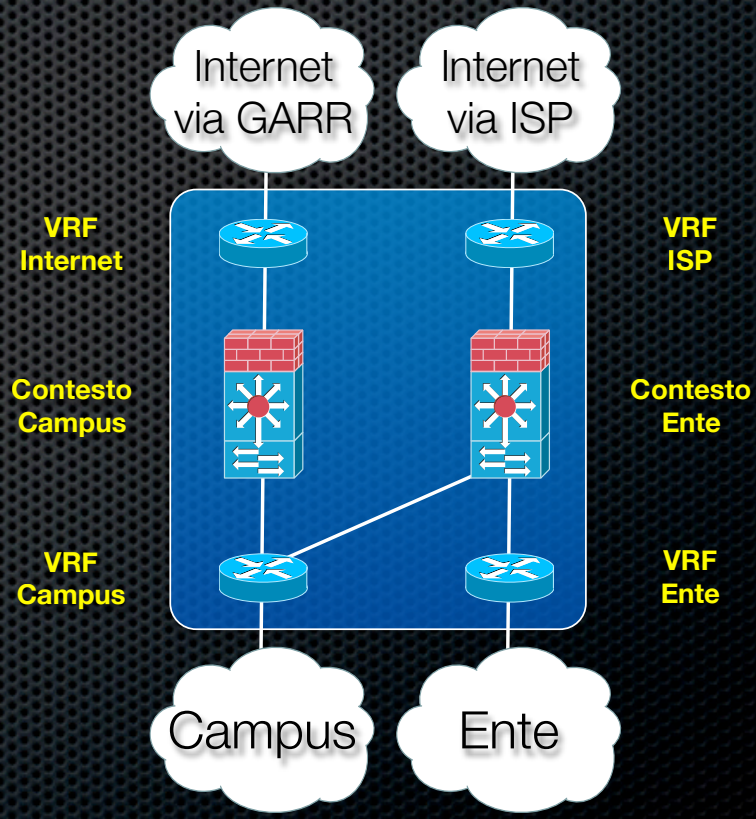
Scenari futuri

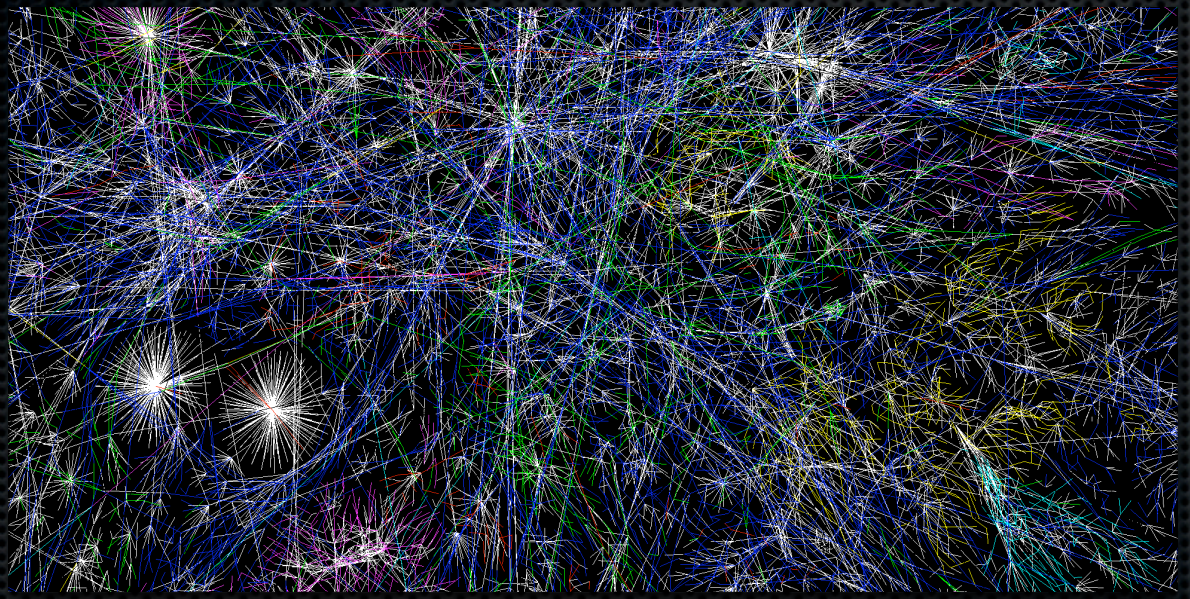
Così come per il router, anche per il firewall possiamo creare e gestire **“contesti” virtuali**.

Ogni contesto rimane separato dagli altri.

Il traffico può essere suddiviso a livello 3 pur utilizzando un’unica rete di trasporto (quella dell’Università) e un unico router di bordo.

In questo ci viene in aiuto la rete **MPLS/BGP**.





Domande e commenti...

dorsale@unisalento.it