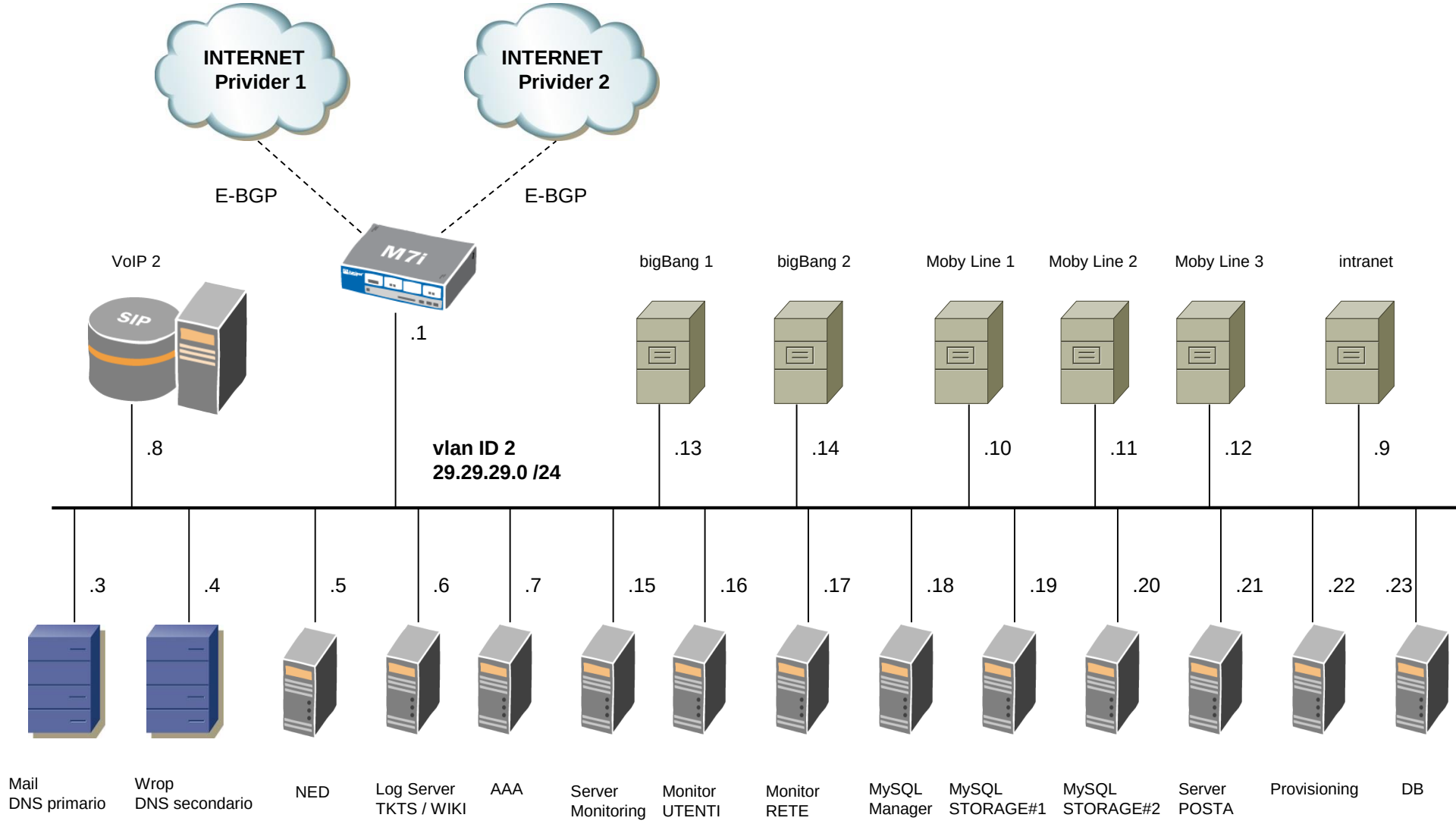
Massimiliano Sbaraglia
Network Engineer

Server Farm with Firewall SSG 520 Juniper

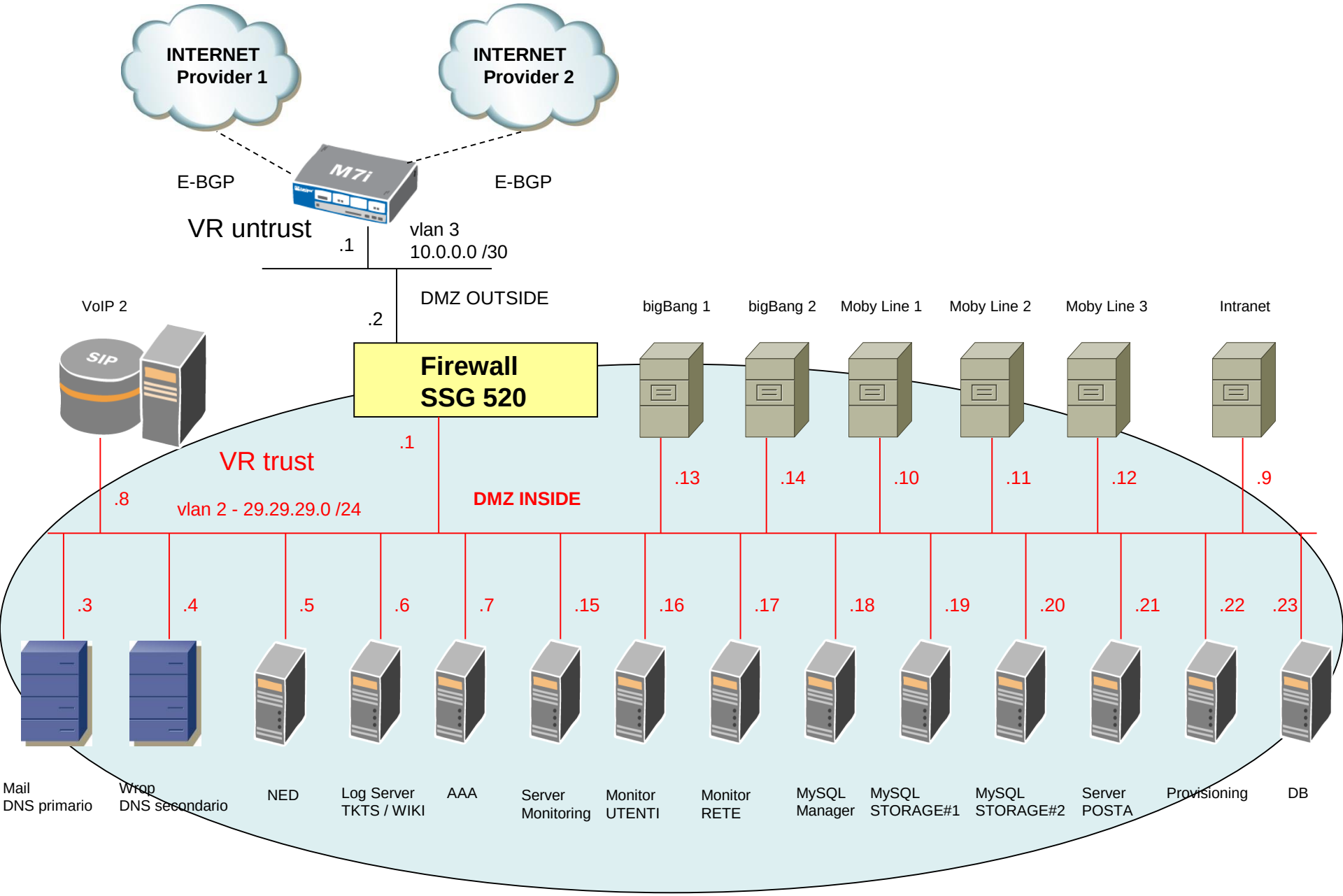
Server Farm Attuale



1^ ipotesi di soluzione : routing IP pubblico on FW

Subnet	Mask	CIDR	Vlan	Area	VR
10.0.0.0	255.255.255.52	/ 30	3	OUTSIDE	untrust
29.29.29.0	255.255.255.0	/ 24	2	INSIDE	trust

1^ ipotesi di soluzione: routing IP pubblico on FW



ZONE to Virtual Router Bindings (1^ ipotesi)

Domain TRUST

trust-vr routing domain

INSIDE

Firewall
SSG 520

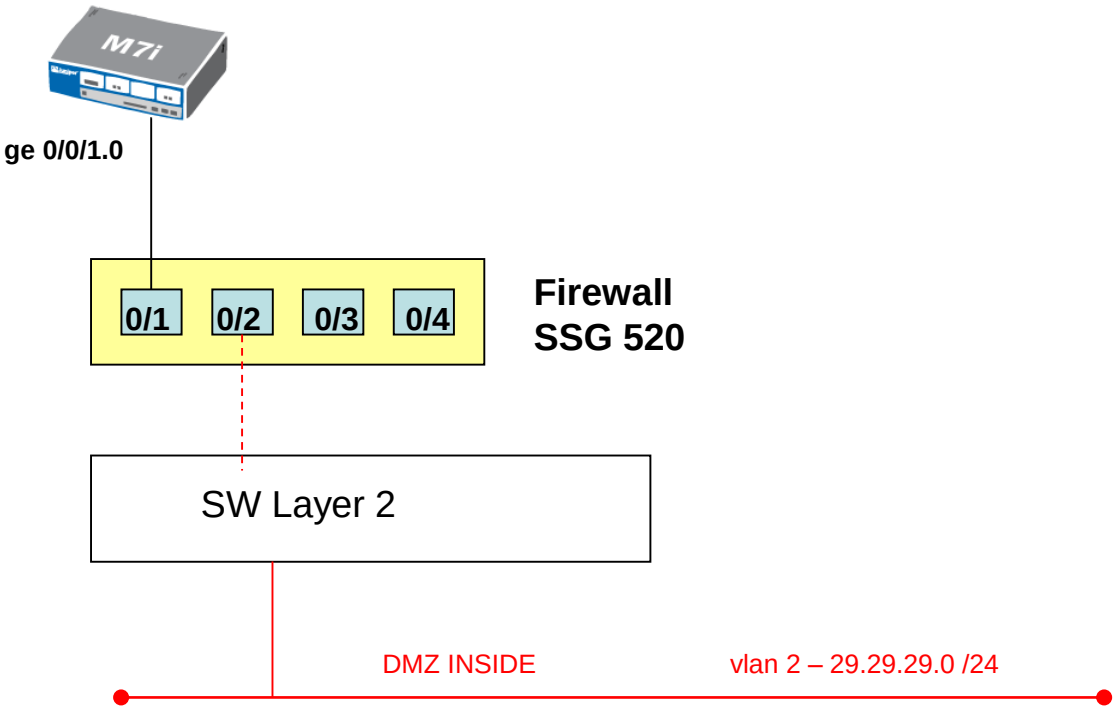
set zone name INSIDE
set zone name OUTSIDE
!
set zone INSIDE vrouter trust-vr
set zone OUTSIDE vrouter untrust-vr

Domain UNTRUST

untrust-vr routing domain

OUTSIDE

Architettura fisica (1^ ipotesi)



Interface to Zone Bindings (1^ ipotesi)

Domain TRUST

trust-vr routing domain

INSIDE
eth 0/2
29.29.29.0 /24
Vlan tag 2

Firewall
SSG 520

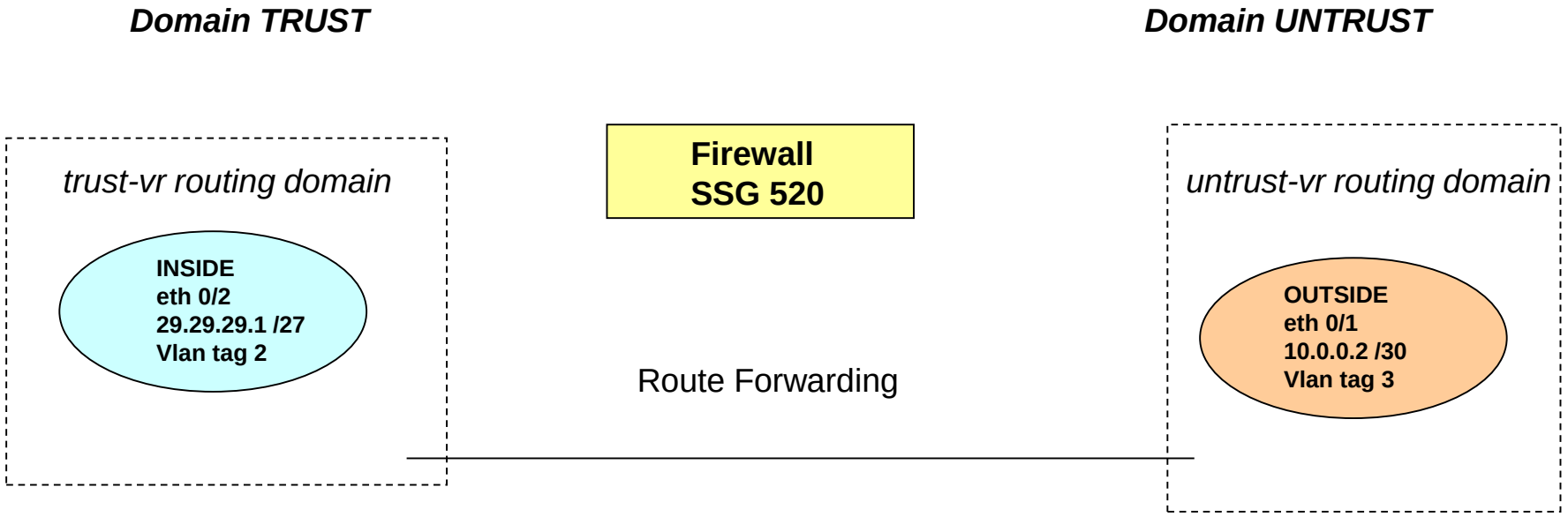
```
set interface ethernet 0/1 zone OUTSIDE
set interface ethernet 0/1 ip 10.0.0.2 /24
set interface ethernet 0/1 manage ping
set interface ethernet 0/1 manage ssh
!
set interface ethernet 0/2 zone INSIDE
set interface ethernet 0/2 ip 29.29.29.1 /24
!
```

Domain UNTRUST

untrust-vr routing domain

OUTSIDE
eth 0/1
10.0.0.0 /30
Vlan tag 3

Routing Domain (1^ ipotesi)



Sul Firewall SSG 520

set vrouter untrust-vr route 0.0.0.0/0 interface ethernet 1/1 gateway 10.0.0.1
set vrouter untrust-vr route 29.29.29.0/24 vrouter trust-vr
!
set vrouter trust-vr route 0.0.0.0/0 vrouter untrust-vr

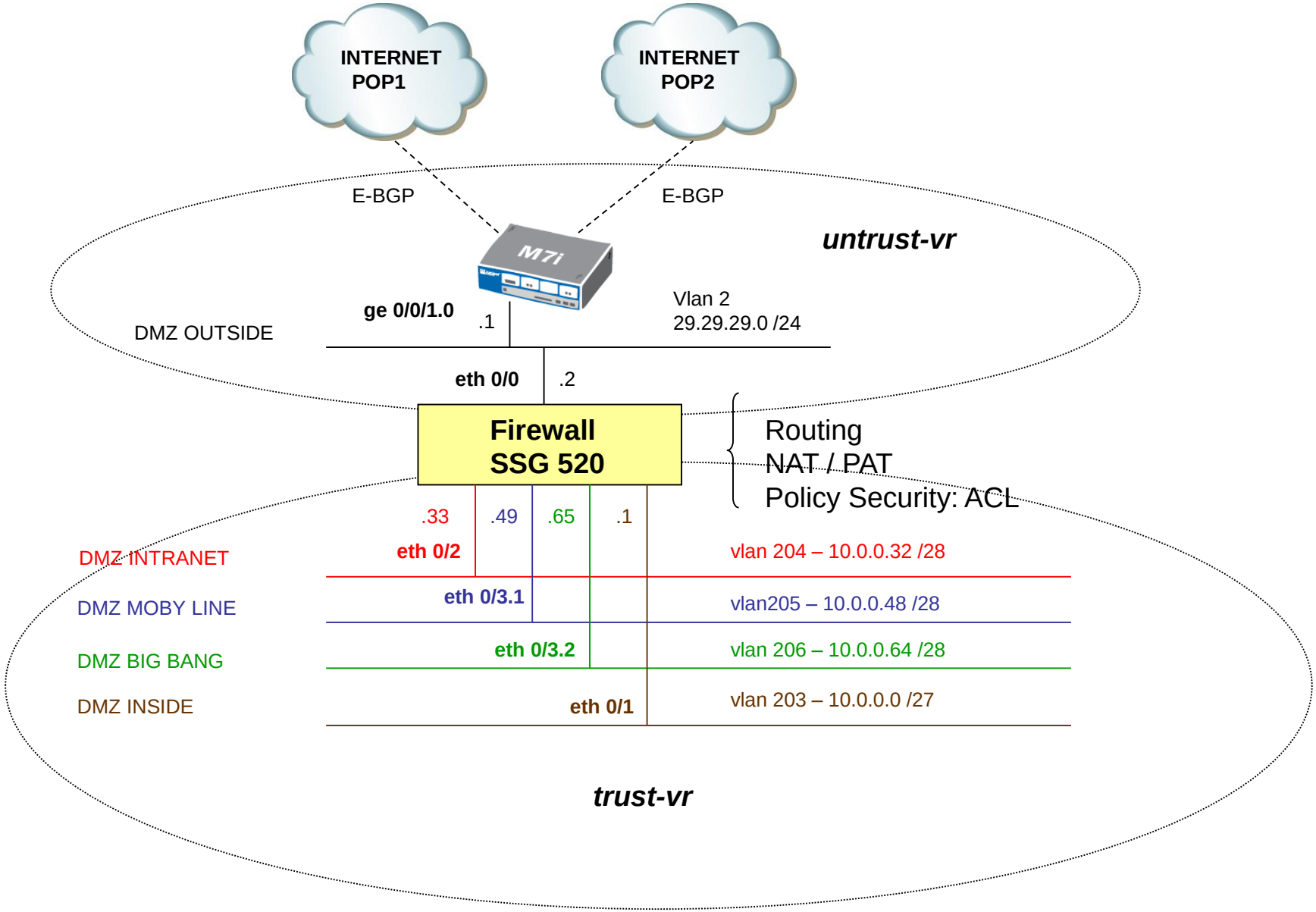
Sul router M7i-01

set route 29.29.29.0 /24 interface ge0/0/1.0 gateway 10.0.0.2

2^ ipotesi di soluzione : IP privato NAT/PAT on FW

Aggregato	Subnet	Mask	CIDR	Vlan	Area	VR
10.10.10.0 /24	**29.29.29.0**	**255.255.255.0**	**/ 24**	**2**	**OUTSIDE**	**untrust**
	10.0.0.32	255.255.255.240	/ 28	204	Intranet	trust
	10.0.0.48	255.255.255.240	/ 28	205	Big Bang	trust
	10.0.0.64	255.255.255.240	/ 28	206	Moby Line	trust
	10.0.0.0	255.255.255.224	/ 27	203	INSIDE	trust

2^ ipotesi di soluzione: IP privato NAT/PAT on FW



ZONE

ZONE:

- OUTSIDE (voip)
- INSIDE
- INTRANET
- MOBY LINE
- BIG BANG

ZONE to Virtual Router Bindings

Domain TRUST

trust-vr routing domain

INSIDE

INTRANET

Moby Line

Big Bang

Firewall
SSG 520

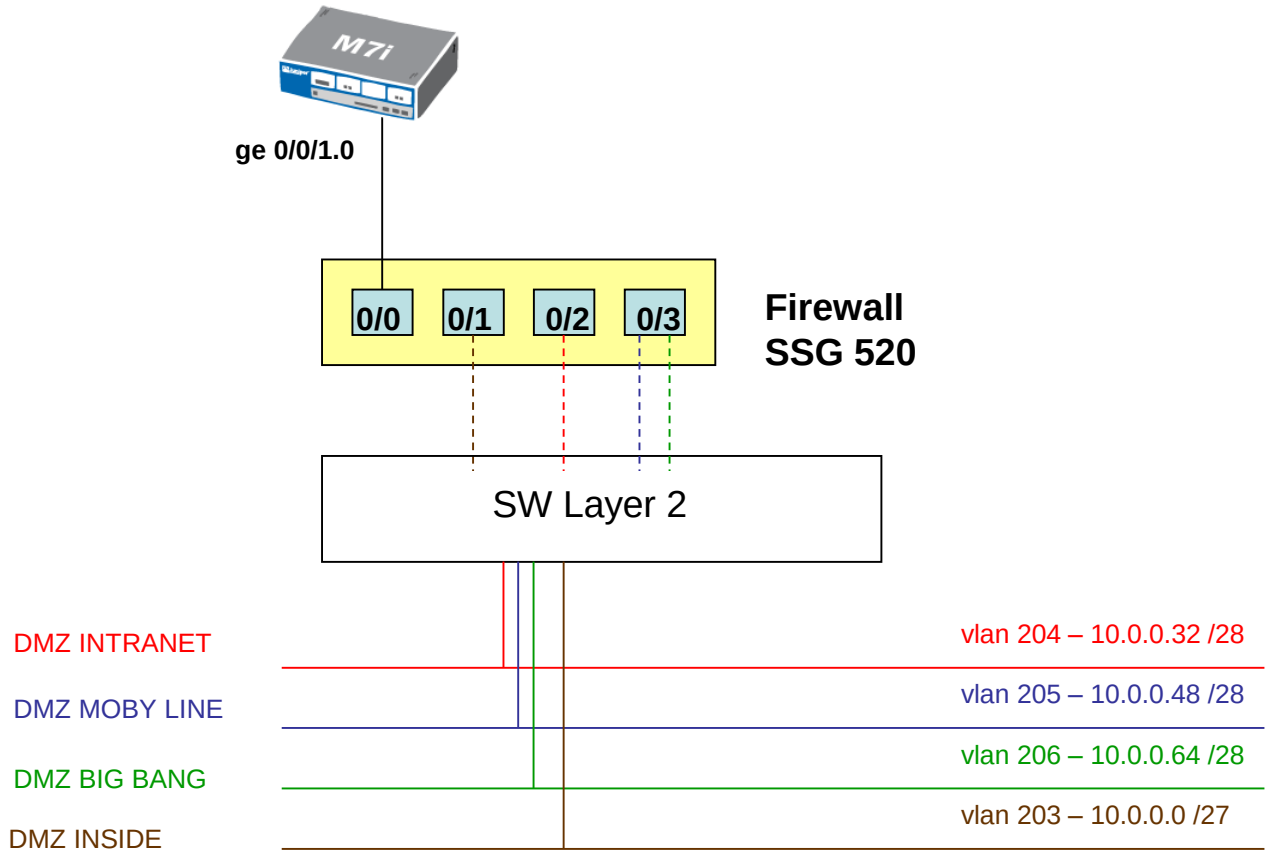
```
set zone name INSIDE
set zone name INTRANET
set zone name MOBYLINE
set zone name BIGBANG
set zone name OUTSIDE
!
set zone INSIDE vrouter trust-vr
set zone INTRANET vrouter trust-vr
set zone MOBYLINE vrouter trust-vr
set zone BIGBANG vrouter trust-vr
set zone OUTSIDE vrouter untrust-vr
```

Domain UNTRUST

untrust-vr routing domain

OUTSIDE

Architettura fisica



Interface to Zone Bindings

Domain TRUST

trust-vr routing domain

INSIDE
eth 0/1
10.0.0.1 /27
Vlan tag 203

INTRANET
eth 0/2
10.0.0.33 /28
Vlan tag 204

Moby Line
eth 0/3.1
10.0.0.49 /28
Vlan tag 205

Big Bang
eth 0/3.2
10.0.0.65 /28
Vlan tag 206

Firewall
SSG 520

```
set interface ethernet 0/0 zone OUTSIDE
set interface ethernet 0/0 ip 29.171.58.2 /24
set interface ethernet 0/0 manage ping
set interface ethernet 0/0 manage ssh
!
set interface ethernet 0/1 zone INSIDE
set interface ethernet 0/1 ip 10.0.0.1 /27
!
set interface ethernet 0/2 zone INTRANET
set interface ethernet 0/2 ip 10.0.0.33 /28
!
set interface ethernet 0/3.1 tag 205 zone MOBYLINE
set interface ethernet 0/3.1 ip 10.0.0.49 /28
!
set interface ethernet 0/3.2 tag 206 zone BIGBANG
set interface ethernet 0/3.2 ip 10.0.0.65 /28
!
```

Domain UNTRUST

untrust-vr routing domain

OUTSIDE
eth 0/0
29.171.58.2 /24
Vlan tag 2

Routing Domain

Domain TRUST

Domain UNTRUST

trust-vr routing domain

INSIDE
eth 0/1
10.0.0.1 /27
Vlan tag 203

INTRANET
eth 0/2
10. 0.0.33 /28
Vlan tag 204

Moby Line
eth 0/3.1
10.0.0.49 /28
Vlan tag 205

Big Bang
eth 0/3.2
10.0.0.65 /28
Vlan tag 206

Firewall
SSG 520

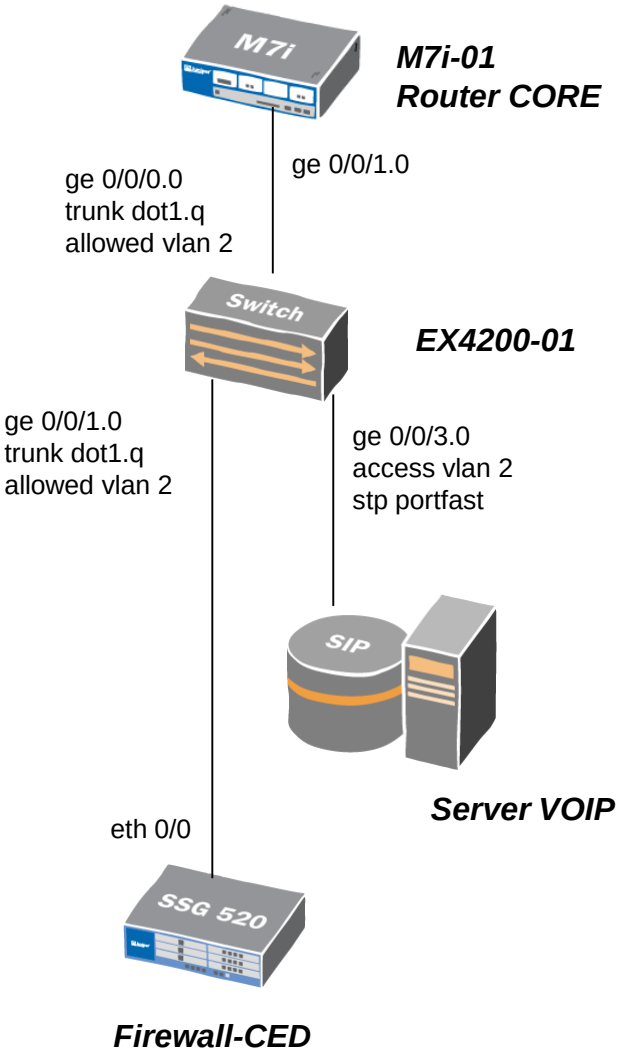
untrust-vr routing domain

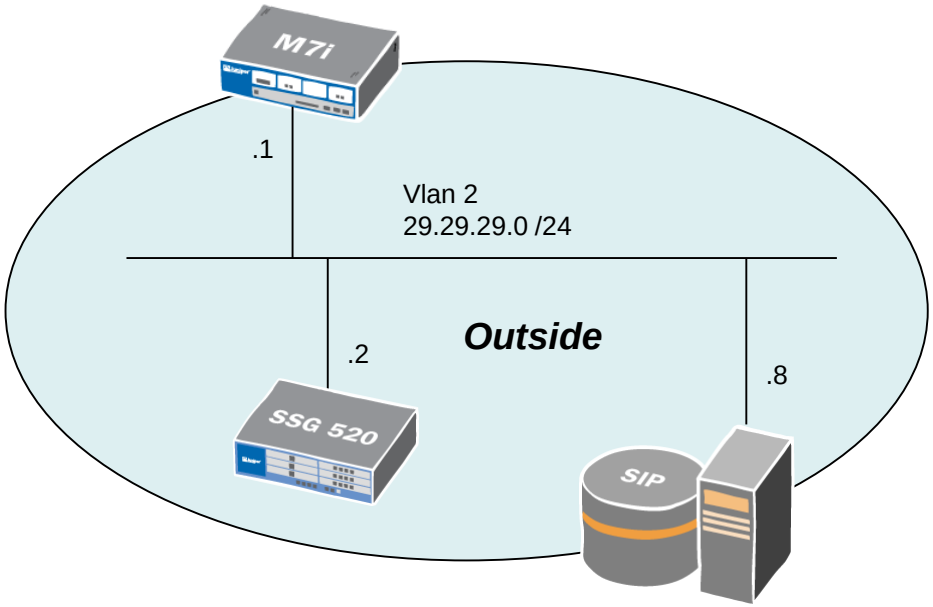
OUTSIDE
eth 0/0
29.29.29.2 /24
Vlan tag 2

set vrouter untrust-vr route 0.0.0.0/0 interface ethernet 0/0 gateway 29.29.29.1
set vrouter untrust-vr route 10.0.0.0/24 vrouter trust-vr
!
set vrouter trust-vr route 0.0.0.0/0 vrouter untrust-vr

Route Forwarding

AREA OUTSIDE (schema fisico e logico)





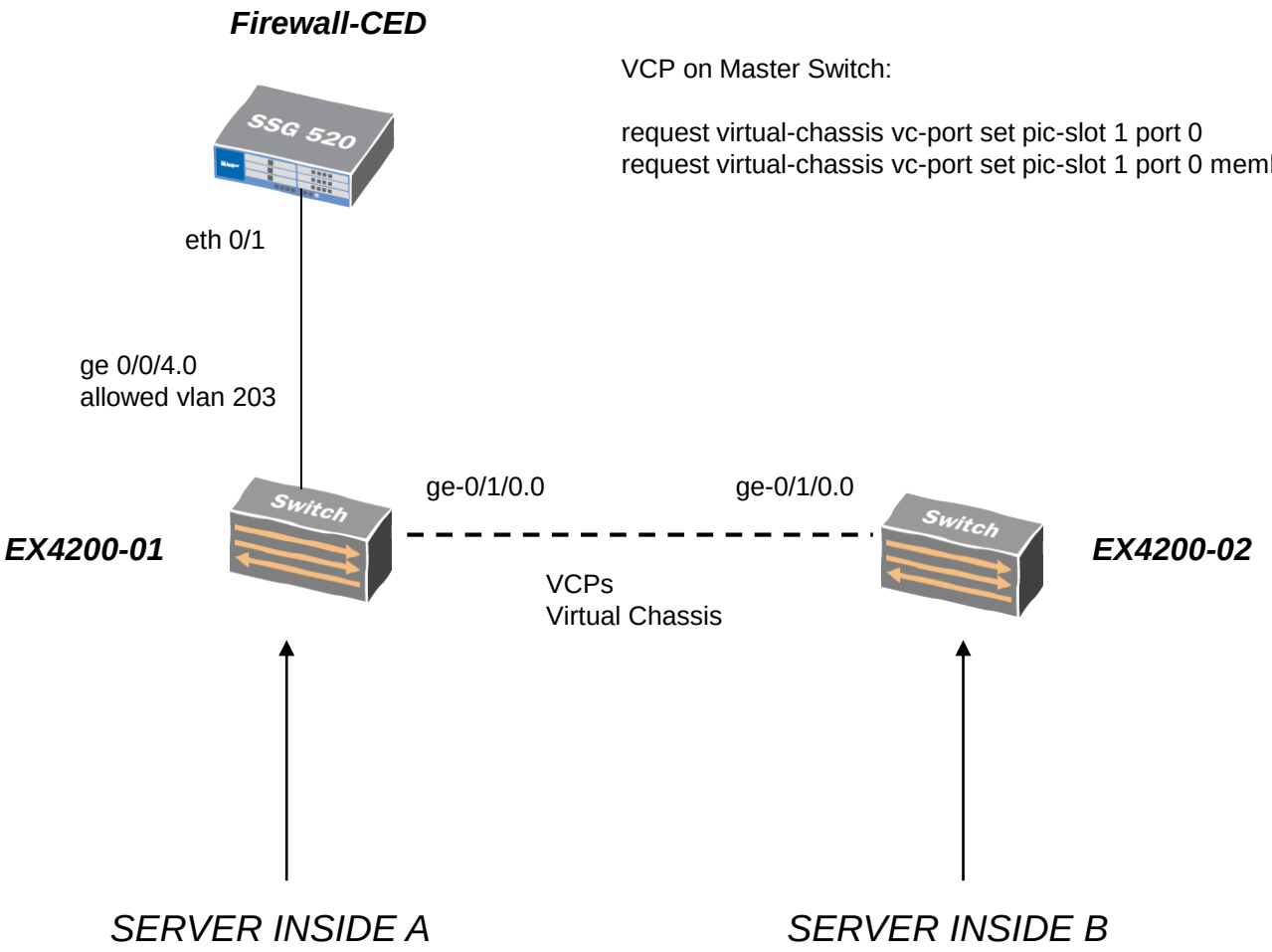
AREA INSIDE (schema fisico)

1. Accendere solo lo switch EX4200-01 (master role)
2. Configurare la masterschip a 255 per lo swith Master
3. Configurare la masterschip sempre a 255 per lo swich Backup (sempre in EX4200-1)

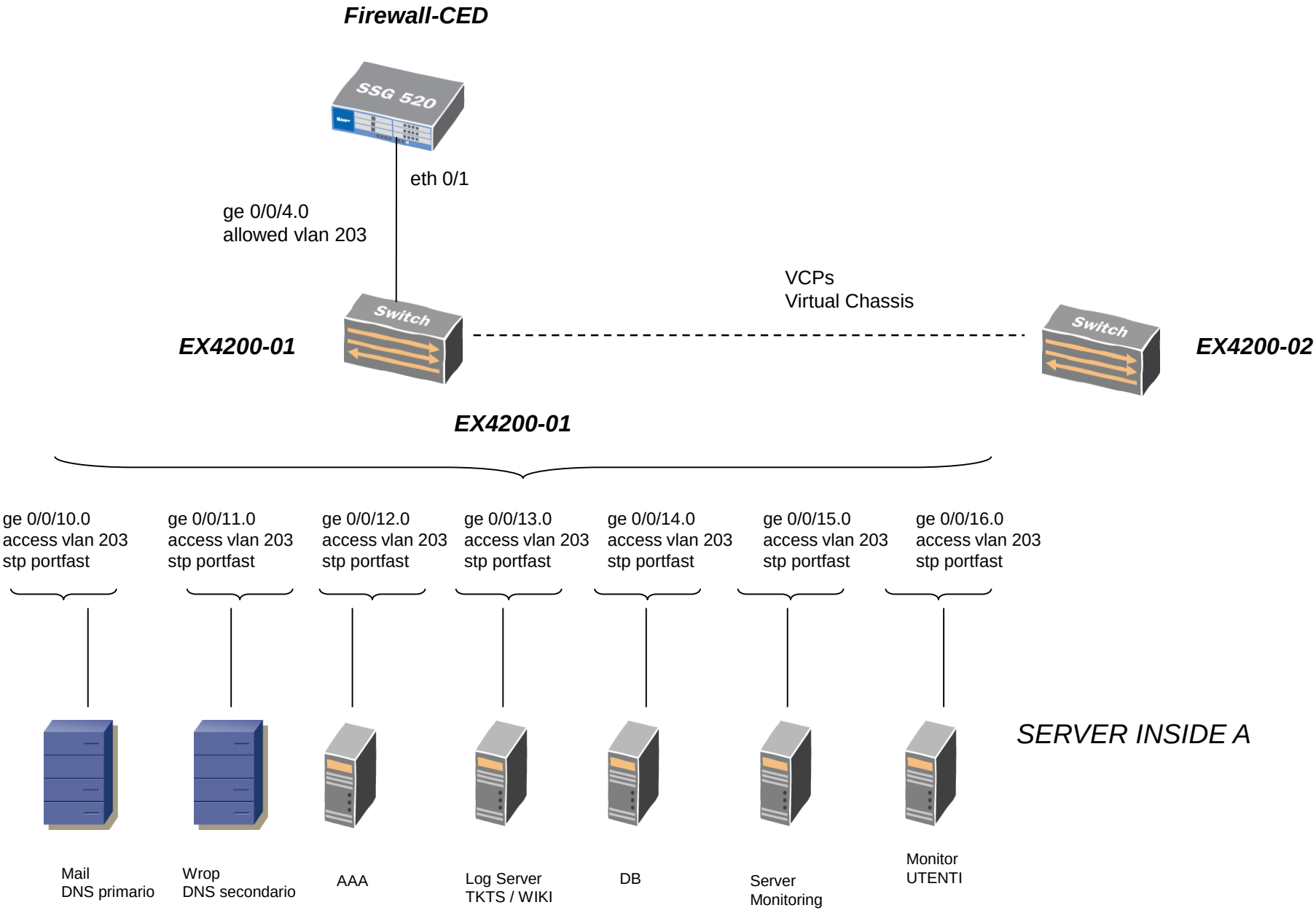
CONFIG:
edit virtual-chassis
set member 0 masterschip-priority 255
set member 1 masterschip-priority 255

VCP on Master Switch:

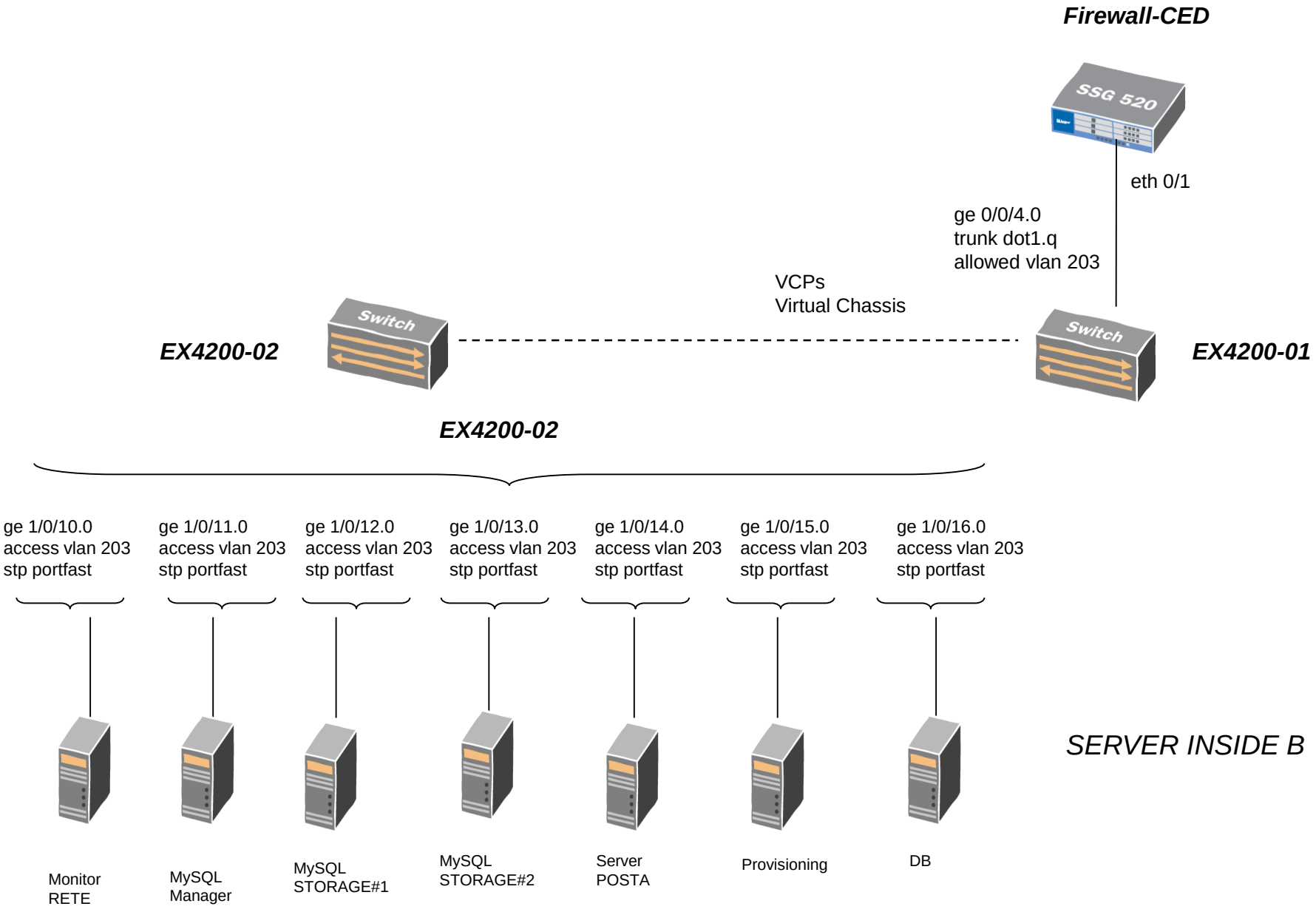
request virtual-chassis vc-port set pic-slot 1 port 0
request virtual-chassis vc-port set pic-slot 1 port 0 membrer 1



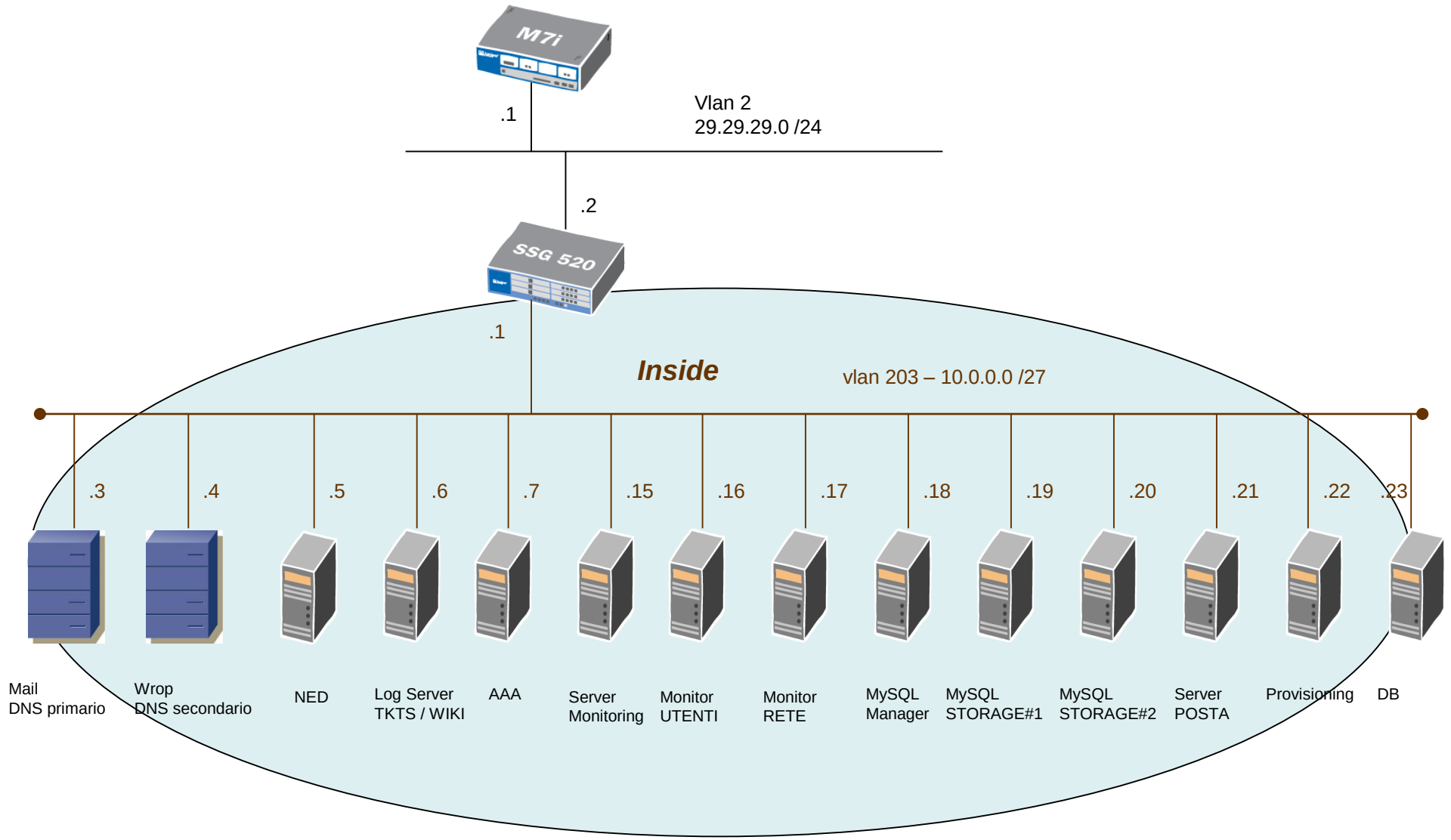
AREA INSIDE (schema fisico SERVER INSIDE A – EX4200-1)



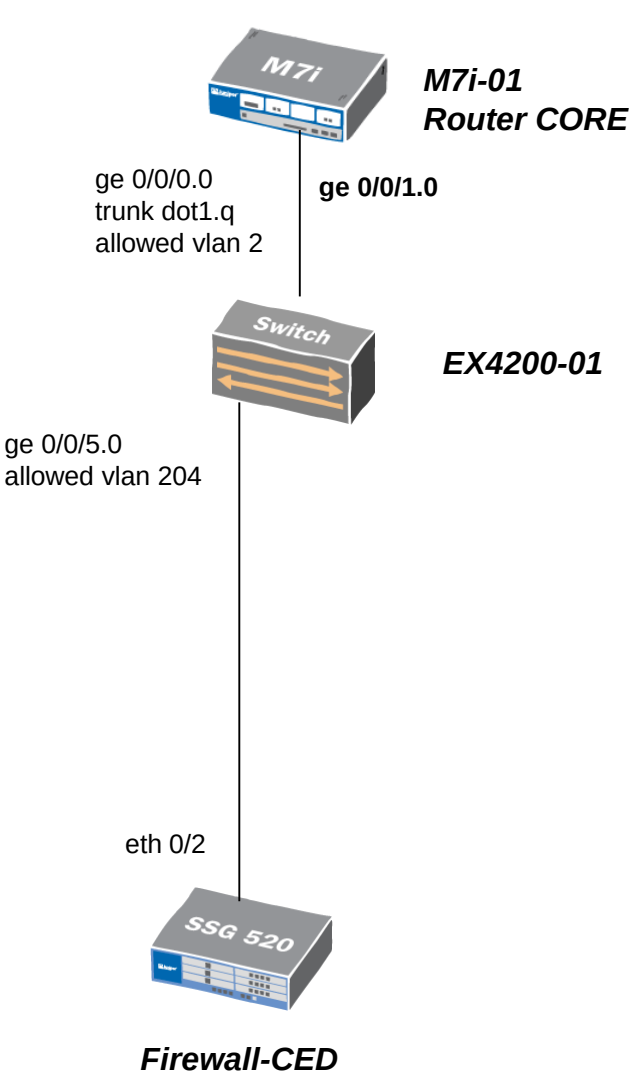
AREA INSIDE (schema fisico SERVER INSIDE B – EX4200-2)

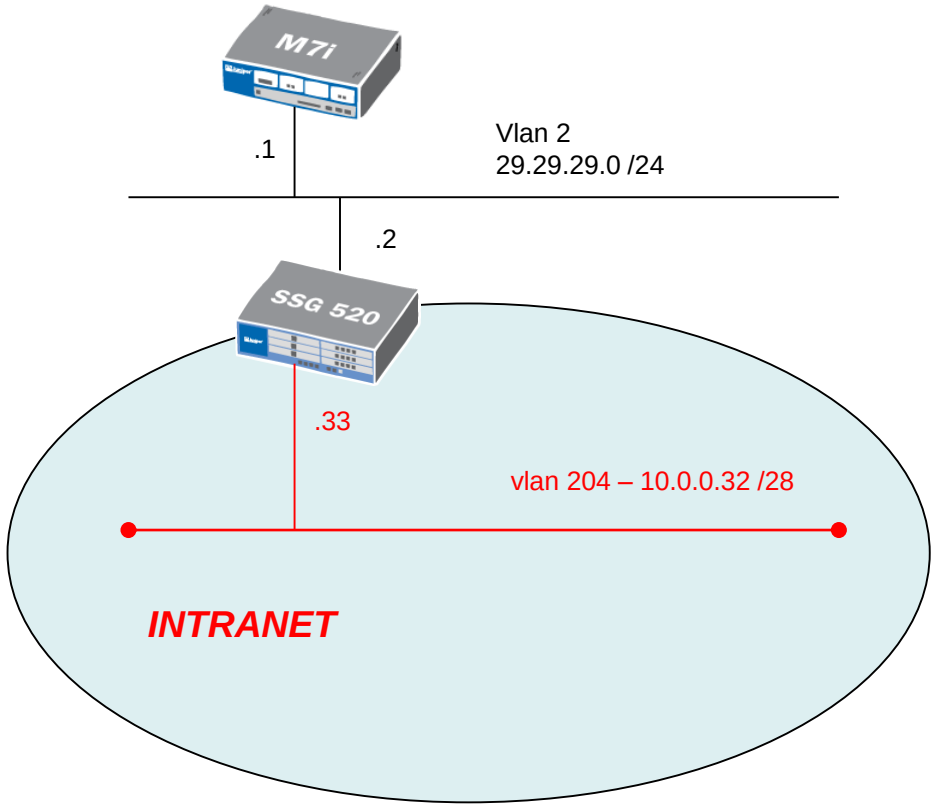


AREA INSIDE (schema logico)

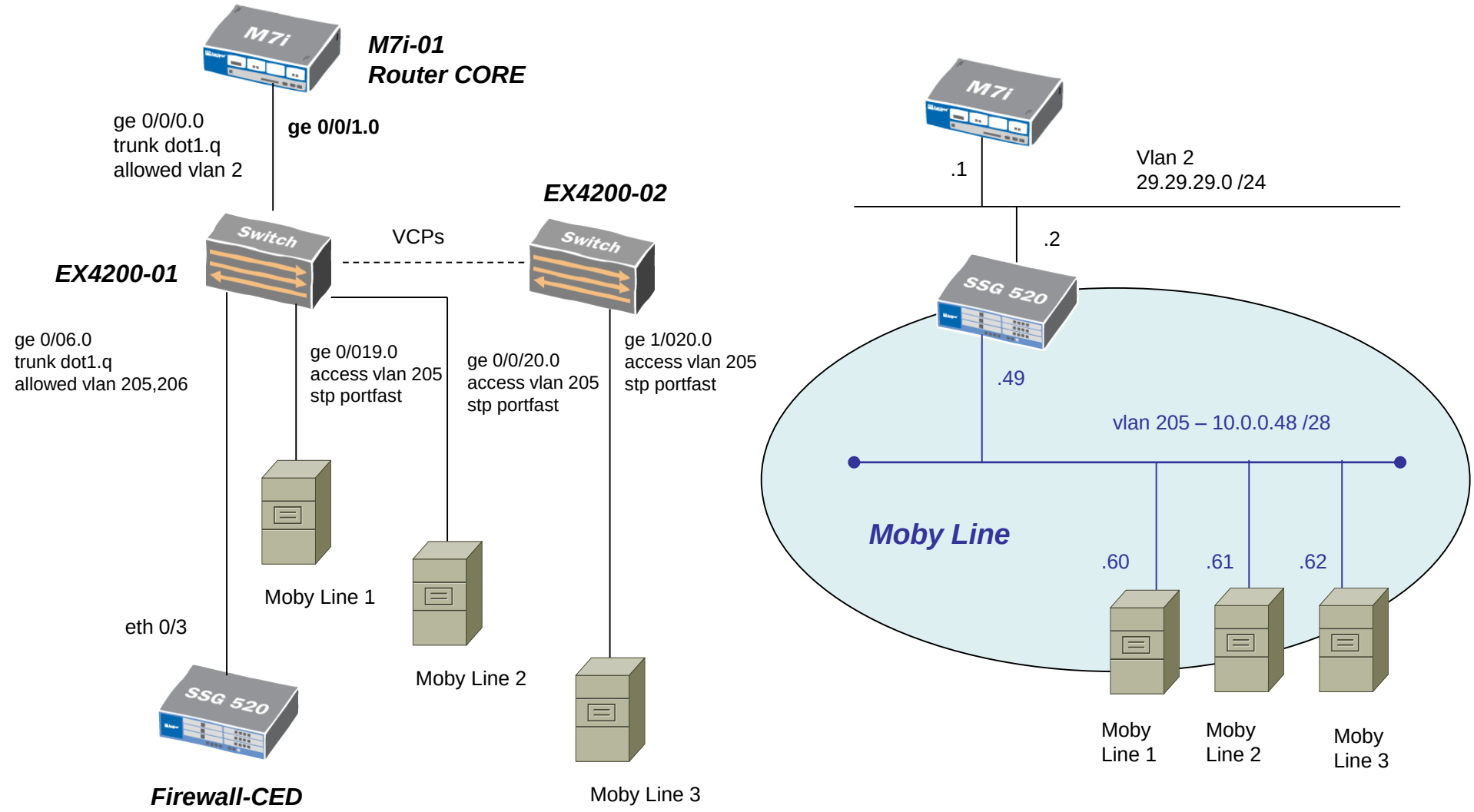


AREA INTRANET (schema fisico e logico)

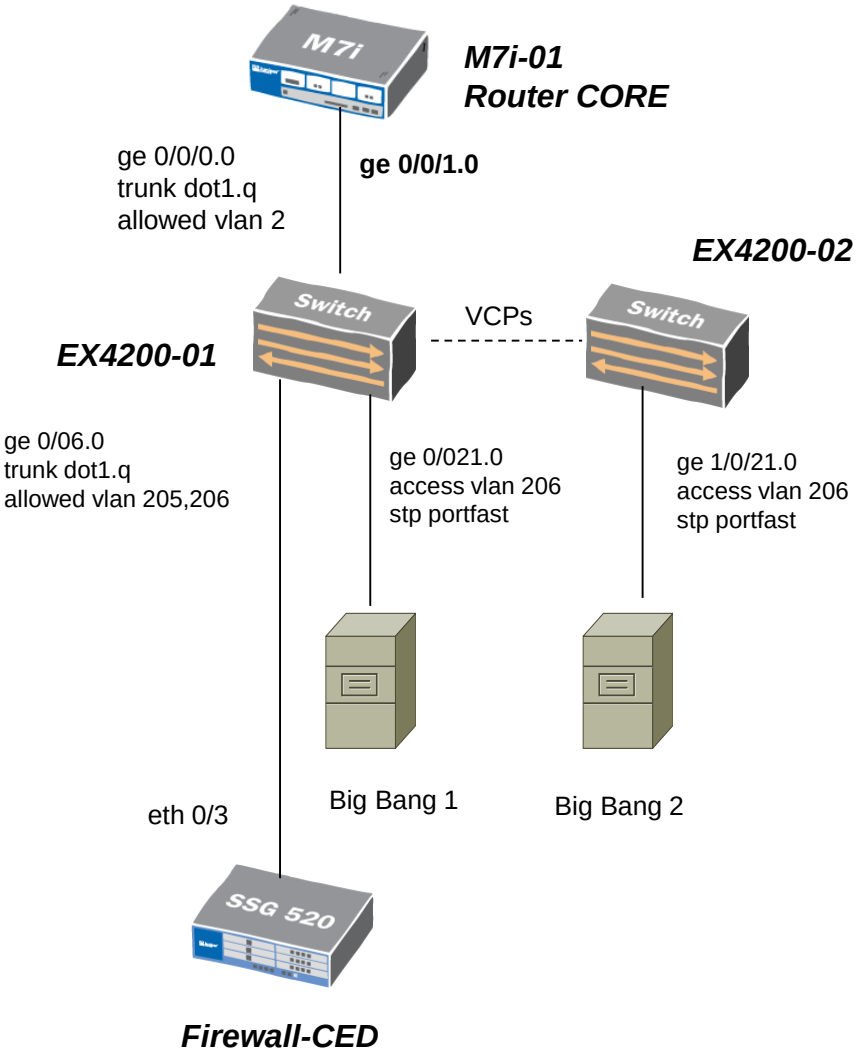


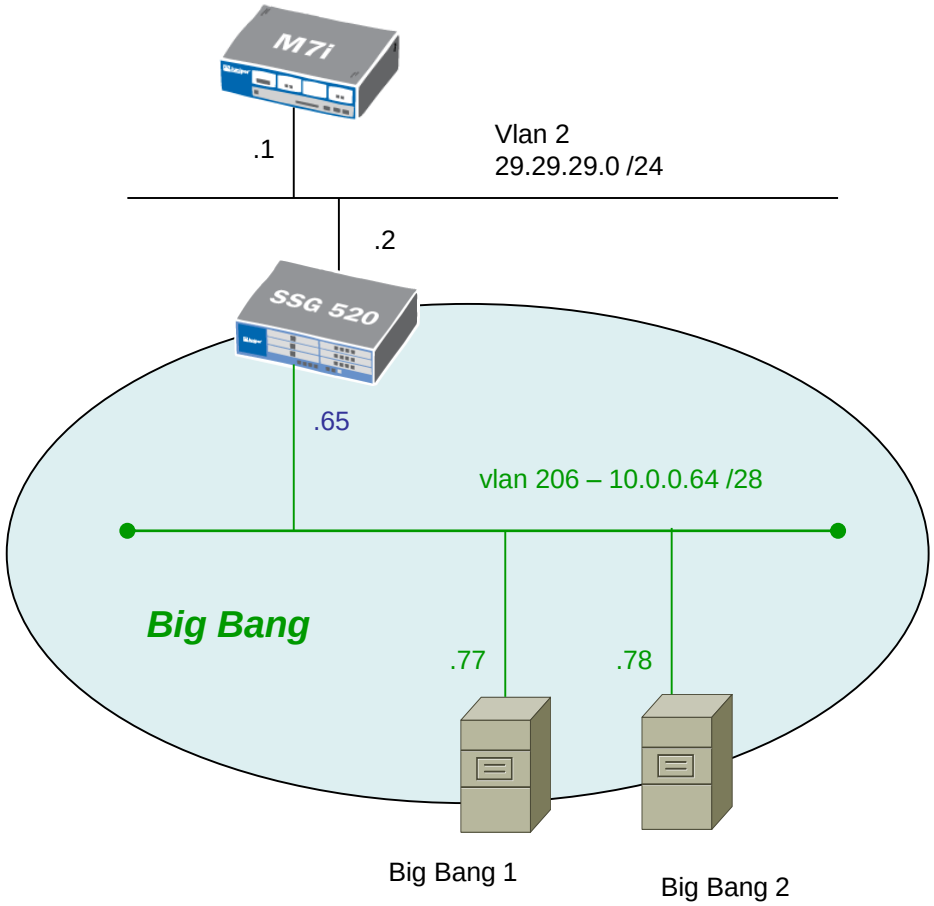


AREA MOBY LINE (schema fisico e logico)

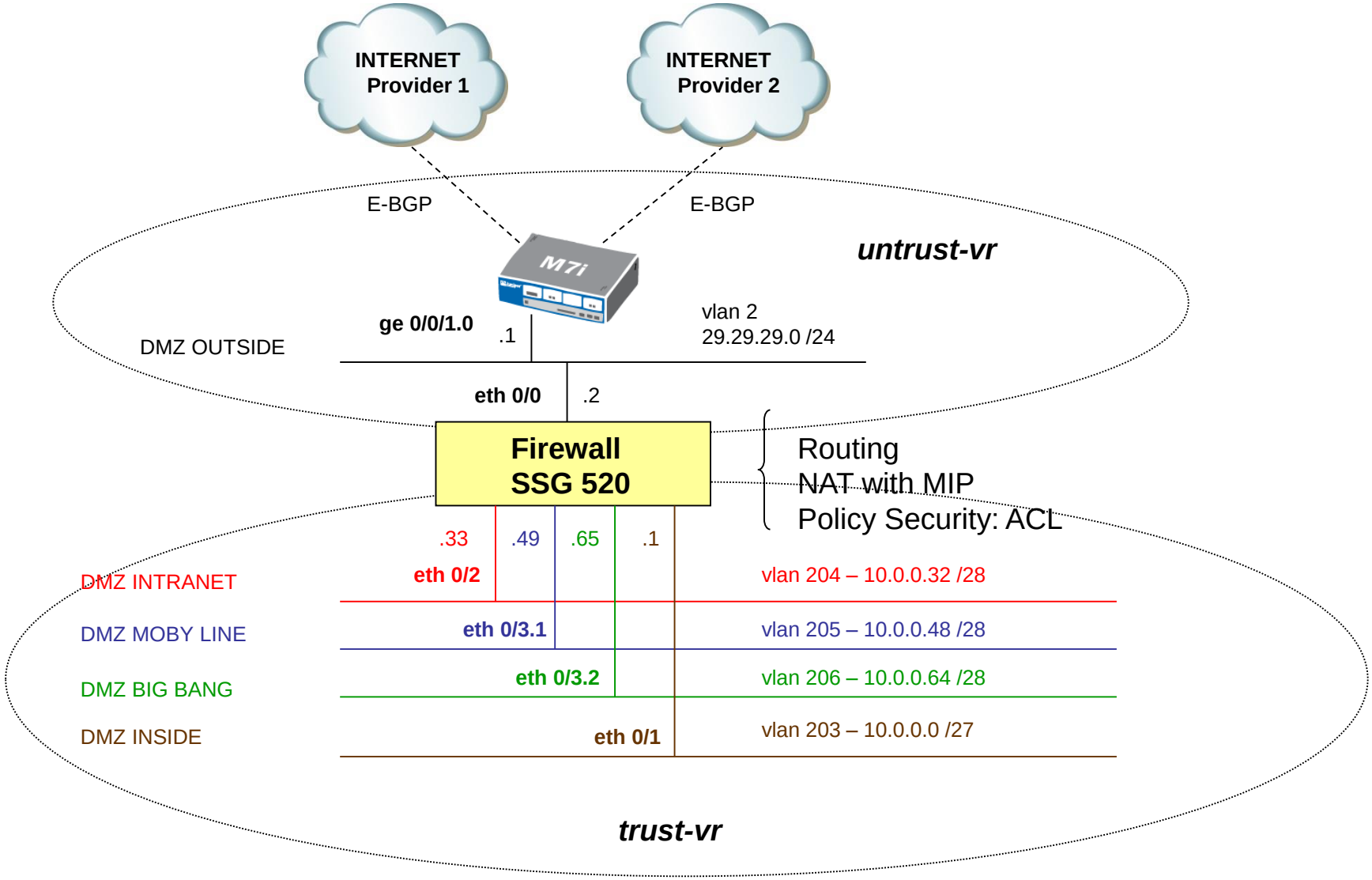


AREA BIG BANG (schema fisico e logico)





MIP on the interface untrust (eth 0/1)



MIP on the untrust interface AREA INSIDE

NAT interface untrust	*NAT interface trust*	*IP eth untrust*	*IP eth trust*	*VR*
eth 0/0	eth 0/1	29.29.29.2 /24	10.0.0.1 /27	TRUST

NAME	*MIP*	*HOST Server*	*Maskera*	*VR*
Mail DNS primrio	29.29.29.3	10.0.0.3	255.255.255.255	TRUST
Wrop DNS secondario	29.29.29.4	10.0.0.4	255.255.255.255	TRUST
NED	29.29.29.5	10.0.0.5	255.255.255.255	TRUST
TKTS WIKI	29.29.29.6	10.0.0.6	255.255.255.255	TRUST
DB1	29.29.29.7	10.0.0.7	255.255.255.255	TRUST
Monitoring	29.29.29.15	10.0.0.15	255.255.255.255	TRUST
Utenti	29.29.29.16	10.0.0.16	255.255.255.255	TRUST
AAA	29.29.29.17	10.0.0.17	255.255.255.255	TRUST
Manager	29.29.29.18	10.0.0.18	255.255.255.255	TRUST
Storage 1	29.29.29.19	10.0.0.19	255.255.255.255	TRUST
Storage 2	29.29.29.20	10.0.0.20	255.255.255.255	TRUST
Posta	29.29.29.21	10.0.0.21	255.255.255.255	TRUST
Provisioning	29.29.29.22	10.0.0.22	255.255.255.255	TRUST
DB	29.29.29.23	10.0.0.23	255.255.255.255	TRUST

NAT with MIP AREA INSIDE (configurazioni)

Domain TRUST

Domain UNTRUST

trust-vr routing domain

INSIDE
eth 0/1
10.0.0.1 /27
Vlan tag 203

Firewall
SSG 520

untrust-vr routing domain

OUTSIDE
eth 0/0
29.29.29.2 /24
Vlan tag 2

interface

set interface ethernet 0/0 zone untrust
set interface ethernet 0/0 ip 29.29.29.2 /24
set interface ethernet 0/1 nat
set interface ethernet 0/1 zone trust
set interface ethernet 0/1 ip 10.0.0.1 /27

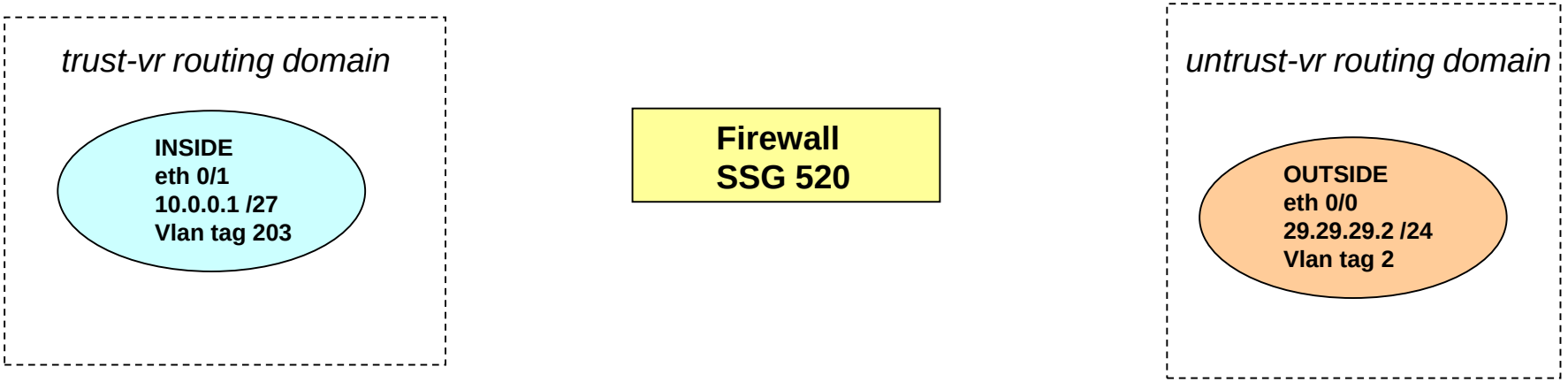
MIP

set interface ethernet0/0 mip 29.29.29.3 host 10.0.0.3 netmask 255.255.255.255 vrouter trust-vr
set interface ethernet0/0 mip 29.29.29.4 host 10.0.0.4 netmask 255.255.255.255 vrouter trust-vr
set interface ethernet0/0 mip 29.29.29.5 host 10.0.0.5 netmask 255.255.255.255 vrouter trust-vr
set interface ethernet0/0 mip 29.29.29.6 host 10.0.0.6 netmask 255.255.255.255 vrouter trust-vr
set interface ethernet0/0 mip 29.29.29.7 host 10.0.0.7 netmask 255.255.255.255 vrouter trust-vr
set interface ethernet0/0 mip 29.29.29.15 host 10.0.0.15 netmask 255.255.255.255 vrouter trust-vr
set interface ethernet0/0 mip 29.29.29.16 host 10.0.0.16 netmask 255.255.255.255 vrouter trust-vr
set interface ethernet0/0 mip 29.29.29.17 host 10.0.0.17 netmask 255.255.255.255 vrouter trust-vr
set interface ethernet0/0 mip 29.29.29.18 host 10.0.0.18 netmask 255.255.255.255 vrouter trust-vr
set interface ethernet0/0 mip 29.29.29.19 host 10.0.0.19 netmask 255.255.255.255 vrouter trust-vr
set interface ethernet0/0 mip 29.29.29.20 host 10.0.0.20 netmask 255.255.255.255 vrouter trust-vr
set interface ethernet0/0 mip 29.29.29.21 host 10.0.0.21 netmask 255.255.255.255 vrouter trust-vr
set interface ethernet0/0 mip 29.29.29.22 host 10.0.0.22 netmask 255.255.255.255 vrouter trust-vr
set interface ethernet0/0 mip 29.29.29.23 host 10.0.0.23 netmask 255.255.255.255 vrouter trust-vr

POLICY AREA INSIDE (configurazioni)

Domain TRUST

Domain UNTRUST



POLICY

set policy from untrust to trust any mip 29.29.29.3 http permit

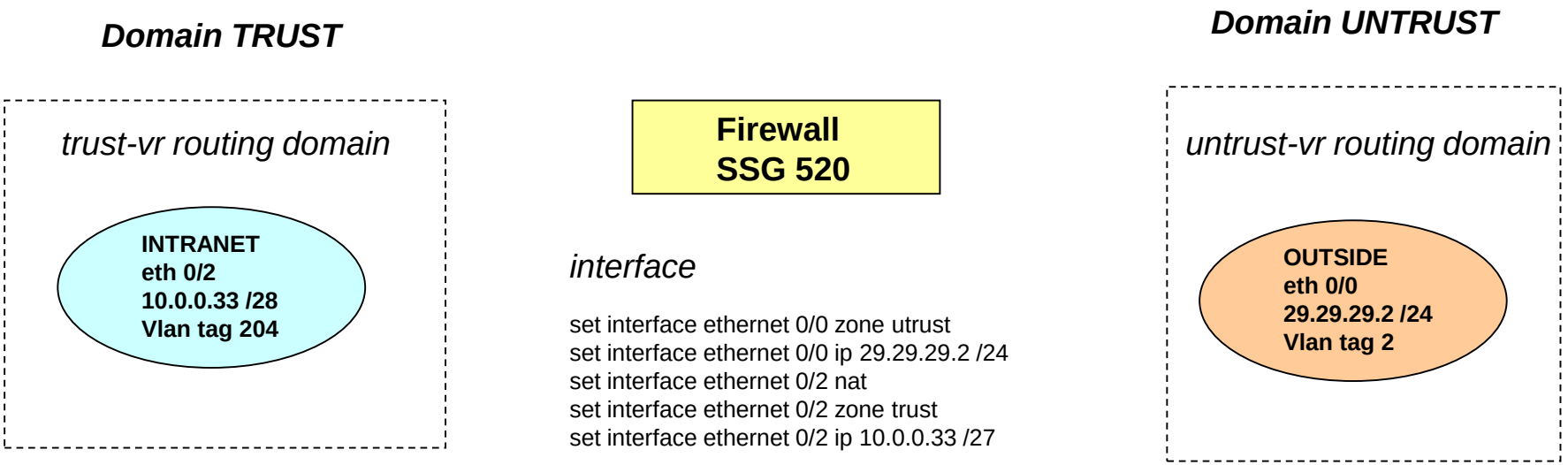
Esempio cisco
access-list acl_out_planet permit tcp host 10.188.38.136 host 10.168.94.94 eq www
!
access-group acl_out_planet in interface outside-PLANET

MIP on the untrust interface AREA NETRESULTS

NAT interface untrust	*NAT interface trust*	*IP eth untrust*	*IP eth trust*	*VR*
eth 0/0	eth 0/2	29.29.29.2 /24	10.0.0.33 /28	TRUST

NAME	*MIP*	*HOST Server*	*Maskera*	*VR*
INTRANET	29.29.29.9	10.0.0.34	255.255.255.255	TRUST

NAT with MIP AREA INTRANET (configurazioni)



interface

set interface ethernet 0/0 zone utrust
set interface ethernet 0/0 ip 29.29.29.2 /24
set interface ethernet 0/2 nat
set interface ethernet 0/2 zone trust
set interface ethernet 0/2 ip 10.0.0.33 /27

MIP

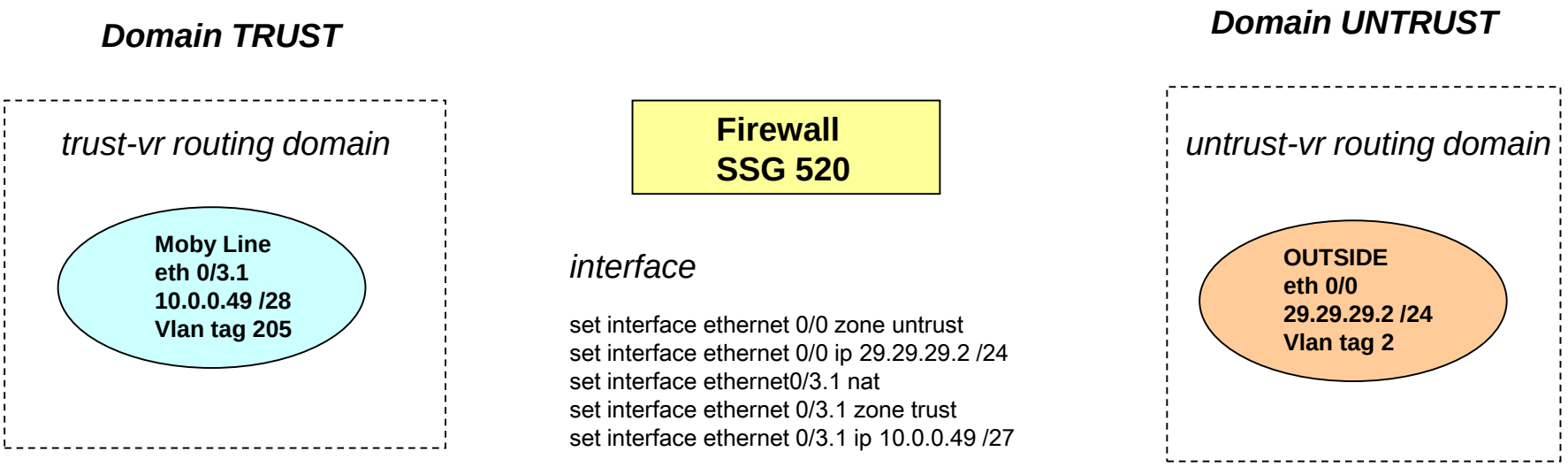
set interface ethernet0/0 mip 29.29.29.9 host 10.0.0.34 netmask 255.255.255.255 vrouter trust-vr

MIP on the untrust interface MOBY LINE

NAT interface untrust	*NAT interface trust*	*IP eth untrust*	*IP eth trust*	*VR*
eth 0/0	eth 0/3.1	29.29.29.2 /24	10.0.0.49 /28	TRUST

NAME	*MIP*	*HOST Server*	*Maskera*	*VR*
MOBY LINE 1	29.29.29.10	10.0.0.50	255.255.255.255	TRUST
MOBY LINE 2	29.29.29.11	10.0.0.51	255.255.255255	TRUST
MOBY LINE 3	29.29.29.12	10.0.0.52	255.255.255.255	TRUST

NAT with MIP AREA MOBY LINE (configurazioni)



interface

```
set interface ethernet 0/0 zone untrust
set interface ethernet 0/0 ip 29.29.29.2 /24
set interface ethernet0/3.1 nat
set interface ethernet 0/3.1 zone trust
set interface ethernet 0/3.1 ip 10.0.0.49 /27
```

MIP

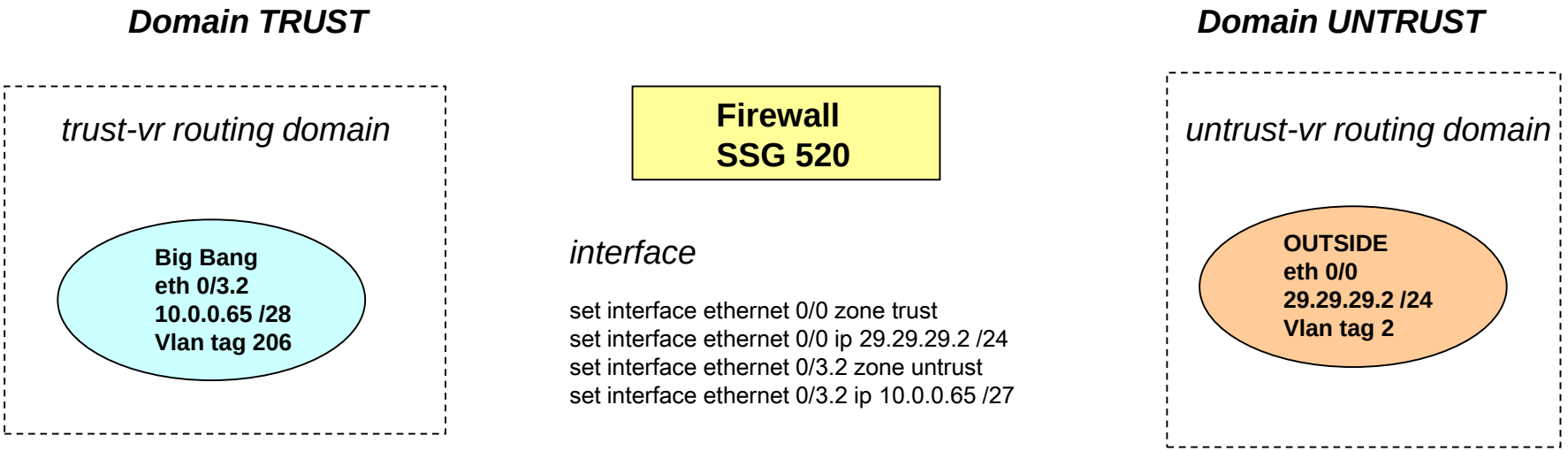
```
set interface ethernet0/0 mip 29.29.29.10 host 10.0.0.50 netmask 255.255.255.255 vrouter trust-vr
set interface ethernet0/0 mip 29.29.29.11 host 10.0.0.51 netmask 255.255.255.255 vrouter trust-vr
set interface ethernet0/0 mip 29.29.29.12 host 10.0.0.52 netmask 255.255.255.255 vrouter trust-vr
```

MIP on the untrust interface BIG BANG

NAT interface untrust	*NAT interface trust*	*IP eth untrust*	*IP eth trust*	*VR*
eth 0/0	eth 0/3.2	29.29.29.2 /24	10.0.0.65 /28	TRUST

NAME	*MIP*	*HOST Server*	*Maskera*	*VR*
BIG BANG 1	29.29.29.13	10.0.0.66	255.255.255.255	TRUST
BIG BANG 2	29.29.29.14	10.0.0.67	255.255.255255	TRUST

NAT with MIP AREA BIG BANG (configurazioni)



interface

set interface ethernet 0/0 zone trust
set interface ethernet 0/0 ip 29.29.29.2 /24
set interface ethernet 0/3.2 zone untrust
set interface ethernet 0/3.2 ip 10.0.0.65 /27

MIP

set interface ethernet0/0 mip 29.29.29.13 host 10.0.0.66 netmask 255.255.255.255 vrouter trust-vr
set interface ethernet0/0 mip 29.29.29.14 host 10.0.0.67 netmask 255.255.255.255 vrouter trust-vr