Secure Networks and Communications
Report Project no 1

Universidade de Aveiro

Sebastian D. González, Mauro Filho

Secure Networks and Communications Report Project no 1

Dept. de Eletrónica, Telecomunicações e Informática

Universidade de Aveiro

sebastian.duque@ua.pt(103690), mauro.filho@ua.pt(103411)

24 de julho de 2024

Conteúdo

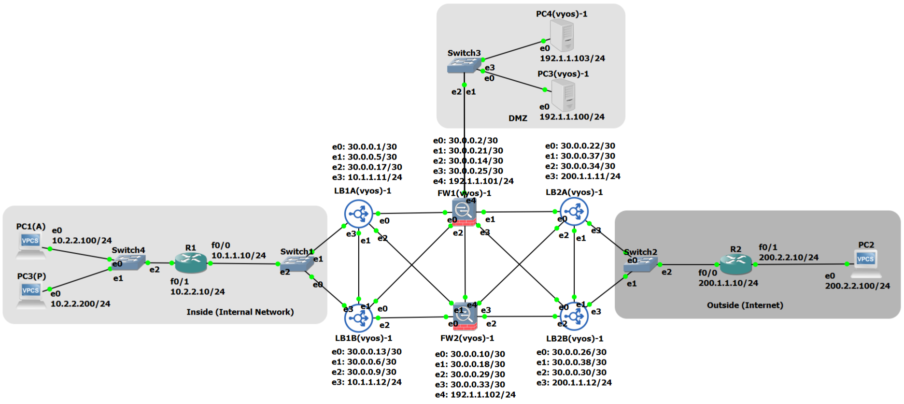
Lista de Figuras

Glossário

DMZ Demilitarized Zone.

Setup geral

1.1 Topologia e Endereços IP



No diagrama acima é possível observar a configuração física dos dispositivos utilizados para a conectividade central do projeto e suas respectivas redes. As redes utilizadas na zona INSIDE são as 10.1.1.0/24 e 10.2.2.0/24, sub-redes de 10.0.0.0/8. Para a zona OUTSIDE temos as redes 200.1.1.0/24 e 200.2.2.0/24, sub-redes de 200.0.0.0/8, finalmente, para a zona DMZ temos a rede 192.1.1.0/24. Todos os restantes endereços foram atribuídos com redes /30.

Firewall Deployment

2.1 Rotas estáticas

As rotas nas firewalls indicam os possíveis caminhos a serem seguidos durante a comunicação entre as redes internas e externas. Aqui exemplificamos a configuração de FW1:

```
set protocols static route 10.2.2.0/24 next-hop 30.0.0.1
set protocols static route 10.2.2.0/24 next-hop 30.0.0.6
set protocols static route 200.2.2.0/24 next-hop 30.0.0.22
set protocols static route 200.2.2.0/24 next-hop 30.0.0.26
```

Listing 2.1: Rotas estáticas FW1

2.2 Definição de Zonas

Nas Firewalls foram configuradas 3 zonas diferentes, a zona **INSIDE**, **Outside** e a Demilitarized Zone (DMZ). Em primeiro lugar, configuramos as interfaces de rede associadas a cada zona. Isto pode ser feito através dos seguintes comandos:

```
set zone-policy zone INSIDE description "Inside (Internal Network)"
set zone-policy zone INSIDE interface eth0
set zone-policy zone INSIDE interface eth2

set zone-policy zone OUTSIDE description "Outside (Internet)"
set zone-policy zone OUTSIDE interface eth1
set zone-policy zone OUTSIDE interface eth3

set zone-policy zone DMZ description 'Dmz'
set zone-policy zone DMZ interface 'eth4'
```

Listing 2.2: Configuração das zonas FW1

2.3 Configuração de mecanismos NAT/PAT

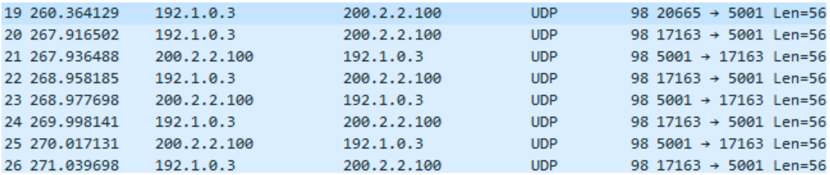
Para ambas as firewalls criámos 2 regras com o objetivo de traduzir endereços IP privados em endereços IP públicos que serão utilizados para comunicar com a internet.
Cada regra especifica um intervalo de endereços de origem e um intervalo correspondente de endereços de tradução e além disso garantimos que os endereços traduzidos não se repetem entre a zona **INSIDE** e **OUTSIDE**.

```
set nat source rule 100 outbound-interface 'eth1'
set nat source rule 100 source address '10.2.2.0/24'
set nat source rule 100 translation address '192.1.0.1-192.1.0.10'

set nat source rule 101 outbound-interface 'eth3'
set nat source rule 101 source address '10.2.2.0/24'
set nat source rule 101 translation address '192.1.0.11-192.1.0.20'
```

Listing 2.3: Configuração de mecanismos NAT/PAT na FW1 e FW2

Como podemos observar na figura 2.1, se fizermos um ping para o **OUTSIDE** a partir da nossa rede interna, é possível observar como de facto a tradução dos ips é efetuada se fizermos uma captura na rede **OUTSIDE**:



```
19 260.364129    192.1.0.3      200.2.2.100    UDP     98 20665 → 5001 Len=56
20 267.916502    192.1.0.3      200.2.2.100    UDP     98 17163 → 5001 Len=56
21 267.936488    200.2.2.100    192.1.0.3      UDP     98 5001 → 17163 Len=56
22 268.958185    192.1.0.3      200.2.2.100    UDP     98 17163 → 5001 Len=56
23 268.977698    200.2.2.100    192.1.0.3      UDP     98 5001 → 17163 Len=56
24 269.998141    192.1.0.3      200.2.2.100    UDP     98 17163 → 5001 Len=56
25 270.017131    200.2.2.100    192.1.0.3      UDP     98 5001 → 17163 Len=56
26 271.039698    192.1.0.3      200.2.2.100    UDP     98 17163 → 5001 Len=56
```

Figura 2.1: Captura entre R2 e PC2

2.4 Políticas e regras para firewalls

Imaginamos o contexto das zonas INSIDE sendo a rede de uma universidade, DMZ sendo uma rede pertencente a universidade que tem serviços que são acedidos por utilizadores na universidade, e OUTSIDE sendo a internet geral. Consideramos também que temos na DMZ os seguintes serviços a correr: HTTP, HTTPS, EMAIL e SSH.
Assim, baseado nestes serviços, definimos as seguintes políticas:

- **HTTP/HTTPS:** Qualquer utilizador pertencente à rede interna deve poder aceder ao serviço na DMZ.
- **EMAIL:** Qualquer utilizador, pertencente à rede interna, deve poder aceder ao serviço na DMZ.

- **SSH:** Qualquer utilizador, pertencente à rede interna, que seja professor, deve poder aceder ao serviço na DMZ.

Para além de garantir apenas acessos autorizados a tais serviços, procuramos também proteger a DMZ contra ataques de DDOS. Assim, configuramos tal comportamento com as seguintes regras em FW1, a configuração em FW2 é feita de forma semelhante:

2.4.1 FROM-INSIDE-TO-DMZ

2.4.1.1 Configuração

Começamos por considerar o caso dos acessos aos serviços HTTP e HTTPS, protocolos TCP. Neste caso, o acesso é feito pelas portas 80 e 443, e sabemos também que o servidor se encontra na máquina PC3, cujo IP é 192.1.1.100. Portanto, para este serviços aceitamos tráfego TCP de INSIDE para DMZ nas portas 80 e 443 cujo endereço de destino é 192.1.1.100:

```
set firewall name FROM-INSIDE-TO-DMZ rule 10 action 'accept'
set firewall name FROM-INSIDE-TO-DMZ rule 10 destination address '192.1.1.100'
set firewall name FROM-INSIDE-TO-DMZ rule 10 destination port '80'
set firewall name FROM-INSIDE-TO-DMZ rule 10 protocol 'tcp'

set firewall name FROM-INSIDE-TO-DMZ rule 20 action 'accept'
set firewall name FROM-INSIDE-TO-DMZ rule 20 destination address '192.1.1.100'
set firewall name FROM-INSIDE-TO-DMZ rule 20 destination port '443'
set firewall name FROM-INSIDE-TO-DMZ rule 20 protocol 'tcp'
```

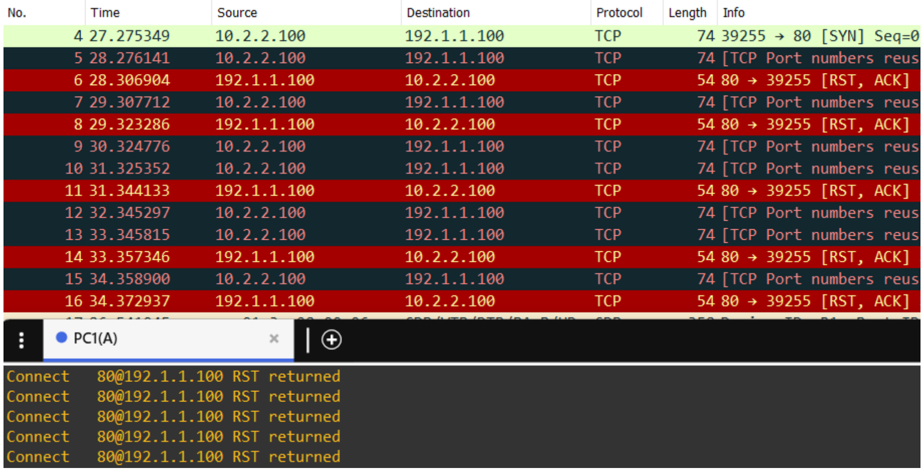
Passando ao serviço de email, consideramos o protocolo de email SMTP, que funciona com a troca de pacotes TCP na porta 25 do servidor. Este servidor, novamente se encontra no PC3. Portanto, para este serviço aceitamos tráfego TCP de INSIDE para DMZ na porta 25 cujo endereço de destino é 192.1.1.100:

```
set firewall name FROM-INSIDE-TO-DMZ rule 30 action 'accept'
set firewall name FROM-INSIDE-TO-DMZ rule 30 destination address '192.1.1.100'
set firewall name FROM-INSIDE-TO-DMZ rule 30 destination port '25'
set firewall name FROM-INSIDE-TO-DMZ rule 30 protocol 'tcp'
```

Finalmente, para o SSH no PC4, queremos apenas aceitar ligações de professores (identificados pela gama de IPs: 10.2.2.200-10.2.2.254). Esta ligação envolve a troca de pacotes TCP na porta 22, e por isso a regra definida aceita tráfego TCP de INSIDE para DMZ na porta 22 cujo endereço de destino é 192.1.1.103, e cujo endereço de origem se encontra na gama indicada:

```
set firewall name FROM-INSIDE-TO-DMZ rule 40 action 'accept'
set firewall name FROM-INSIDE-TO-DMZ rule 40 destination address '192.1.1.103'
set firewall name FROM-INSIDE-TO-DMZ rule 40 destination port '22'
set firewall name FROM-INSIDE-TO-DMZ rule 40 protocol 'tcp'
set firewall name FROM-INSIDE-TO-DMZ rule 40 source address '10.2.2.200-10.2.2.254'
```

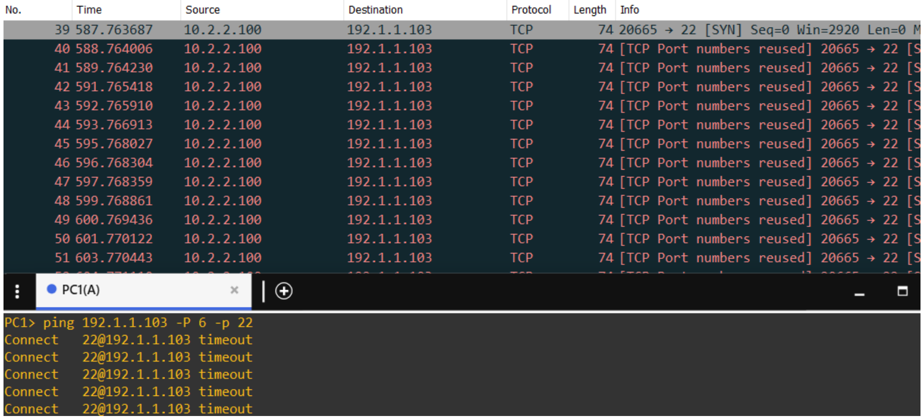
2.4.1.2 Teste



No.	Time	Source	Destination	Protocol	Length	Info
4	27.275349	10.2.2.100	192.1.1.100	TCP	74	39255 → 80 [SYN] Seq=0
5	28.276141	10.2.2.100	192.1.1.100	TCP	74	[TCP Port numbers reus
6	28.306904	192.1.1.100	10.2.2.100	TCP	54	80 → 39255 [RST, ACK]
7	29.307712	10.2.2.100	192.1.1.100	TCP	74	[TCP Port numbers reus
8	29.323286	192.1.1.100	10.2.2.100	TCP	54	80 → 39255 [RST, ACK]
9	30.324776	10.2.2.100	192.1.1.100	TCP	74	[TCP Port numbers reus
10	31.325352	10.2.2.100	192.1.1.100	TCP	74	[TCP Port numbers reus
11	31.344133	192.1.1.100	10.2.2.100	TCP	54	80 → 39255 [RST, ACK]
12	32.345297	10.2.2.100	192.1.1.100	TCP	74	[TCP Port numbers reus
13	33.345815	10.2.2.100	192.1.1.100	TCP	74	[TCP Port numbers reus
14	33.357346	192.1.1.100	10.2.2.100	TCP	54	80 → 39255 [RST, ACK]
15	34.358900	10.2.2.100	192.1.1.100	TCP	74	[TCP Port numbers reus
16	34.372937	192.1.1.100	10.2.2.100	TCP	54	80 → 39255 [RST, ACK]

```
Connect   80@192.1.1.100 RST returned
Connect   80@192.1.1.100 RST returned
Connect   80@192.1.1.100 RST returned
Connect   80@192.1.1.100 RST returned
Connect   80@192.1.1.100 RST returned
```

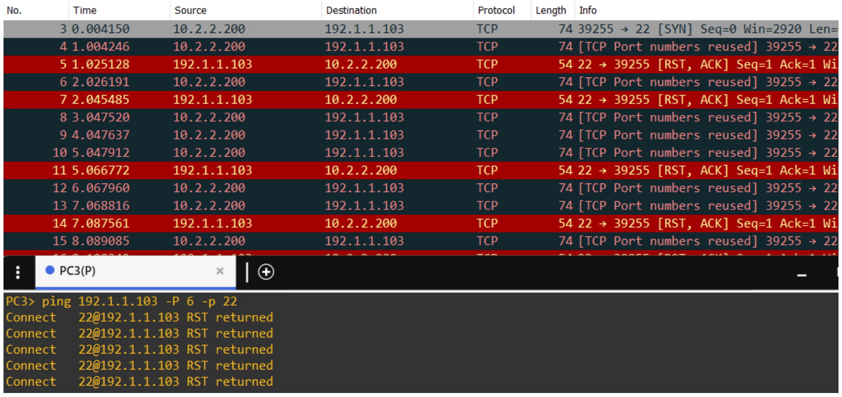
Figura 2.2: Ping TCP do PC1 (aluno) para a HTTP na DMZ com sucesso. Pacotes capturados entre PC1 e Switch4



No.	Time	Source	Destination	Protocol	Length	Info
39	587.763687	10.2.2.100	192.1.1.103	TCP	74	20665 → 22 [SYN] Seq=0 Win=2920 Len=0 M
40	588.764006	10.2.2.100	192.1.1.103	TCP	74	[TCP Port numbers reused] 20665 → 22 [S
41	589.764230	10.2.2.100	192.1.1.103	TCP	74	[TCP Port numbers reused] 20665 → 22 [S
42	591.765418	10.2.2.100	192.1.1.103	TCP	74	[TCP Port numbers reused] 20665 → 22 [S
43	592.765910	10.2.2.100	192.1.1.103	TCP	74	[TCP Port numbers reused] 20665 → 22 [S
44	593.766913	10.2.2.100	192.1.1.103	TCP	74	[TCP Port numbers reused] 20665 → 22 [S
45	595.768027	10.2.2.100	192.1.1.103	TCP	74	[TCP Port numbers reused] 20665 → 22 [S
46	596.768304	10.2.2.100	192.1.1.103	TCP	74	[TCP Port numbers reused] 20665 → 22 [S
47	597.768359	10.2.2.100	192.1.1.103	TCP	74	[TCP Port numbers reused] 20665 → 22 [S
48	599.768861	10.2.2.100	192.1.1.103	TCP	74	[TCP Port numbers reused] 20665 → 22 [S
49	600.769436	10.2.2.100	192.1.1.103	TCP	74	[TCP Port numbers reused] 20665 → 22 [S
50	601.770122	10.2.2.100	192.1.1.103	TCP	74	[TCP Port numbers reused] 20665 → 22 [S
51	603.770443	10.2.2.100	192.1.1.103	TCP	74	[TCP Port numbers reused] 20665 → 22 [S

```
PC1> ping 192.1.1.103 -P 6 -p 22
Connect   22@192.1.1.103 timeout
Connect   22@192.1.1.103 timeout
Connect   22@192.1.1.103 timeout
Connect   22@192.1.1.103 timeout
Connect   22@192.1.1.103 timeout
```

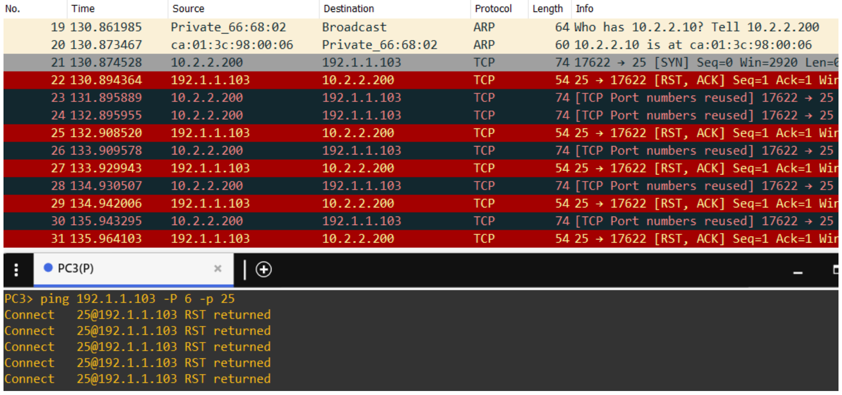
Figura 2.3: Ping TCP do PC1 (aluno) para SSH na DMZ sem sucesso. Pacotes capturados entre PC1 e Switch4



No.	Time	Source	Destination	Protocol	Length	Info
3	0.004150	10.2.2.200	192.1.1.103	TCP	74	39255 → 22 [SYN] Seq=0 Win=2920 Len=
4	1.004246	10.2.2.200	192.1.1.103	TCP	74	[TCP Port numbers reused] 39255 → 22
5	1.025128	192.1.1.103	10.2.2.200	TCP	54	22 → 39255 [RST, ACK] Seq=1 Ack=1 Wi
6	2.026191	10.2.2.200	192.1.1.103	TCP	74	[TCP Port numbers reused] 39255 → 22
7	2.045485	192.1.1.103	10.2.2.200	TCP	54	22 → 39255 [RST, ACK] Seq=1 Ack=1 Wi
8	3.047520	10.2.2.200	192.1.1.103	TCP	74	[TCP Port numbers reused] 39255 → 22
9	4.047637	10.2.2.200	192.1.1.103	TCP	74	[TCP Port numbers reused] 39255 → 22
10	5.047912	10.2.2.200	192.1.1.103	TCP	74	[TCP Port numbers reused] 39255 → 22
11	5.066772	192.1.1.103	10.2.2.200	TCP	54	22 → 39255 [RST, ACK] Seq=1 Ack=1 Wi
12	6.067960	10.2.2.200	192.1.1.103	TCP	74	[TCP Port numbers reused] 39255 → 22
13	7.068816	10.2.2.200	192.1.1.103	TCP	74	[TCP Port numbers reused] 39255 → 22
14	7.087561	192.1.1.103	10.2.2.200	TCP	54	22 → 39255 [RST, ACK] Seq=1 Ack=1 Wi
15	8.089085	10.2.2.200	192.1.1.103	TCP	74	[TCP Port numbers reused] 39255 → 22

```
PC3> ping 192.1.1.103 -P 6 -p 22
Connect   22@192.1.1.103 RST returned
Connect   22@192.1.1.103 RST returned
Connect   22@192.1.1.103 RST returned
Connect   22@192.1.1.103 RST returned
Connect   22@192.1.1.103 RST returned
```

Figura 2.4: Ping TCP do PC3 (professor) para SSH na DMZ com sucesso. Pacotes capturados entre PC3 e Switch4



No.	Time	Source	Destination	Protocol	Length	Info
19	130.861985	Private_66:68:02	Broadcast	ARP	64	Who has 10.2.2.10? Tell 10.2.2.200
20	130.873467	ca:01:3c:98:00:06	Private_66:68:02	ARP	60	10.2.2.10 is at ca:01:3c:98:00:06
21	130.874528	10.2.2.200	192.1.1.103	TCP	74	17622 → 25 [SYN] Seq=0 Win=2920 Len=0
22	130.894364	192.1.1.103	10.2.2.200	TCP	54	25 → 17622 [RST, ACK] Seq=1 Ack=1 Win
23	131.895889	10.2.2.200	192.1.1.103	TCP	74	[TCP Port numbers reused] 17622 → 25
24	132.895955	10.2.2.200	192.1.1.103	TCP	74	[TCP Port numbers reused] 17622 → 25
25	132.908520	192.1.1.103	10.2.2.200	TCP	54	25 → 17622 [RST, ACK] Seq=1 Ack=1 Win
26	133.909578	10.2.2.200	192.1.1.103	TCP	74	[TCP Port numbers reused] 17622 → 25
27	133.929943	192.1.1.103	10.2.2.200	TCP	54	25 → 17622 [RST, ACK] Seq=1 Ack=1 Win
28	134.930507	10.2.2.200	192.1.1.103	TCP	74	[TCP Port numbers reused] 17622 → 25
29	134.942006	192.1.1.103	10.2.2.200	TCP	54	25 → 17622 [RST, ACK] Seq=1 Ack=1 Win
30	135.943295	10.2.2.200	192.1.1.103	TCP	74	[TCP Port numbers reused] 17622 → 25
31	135.964103	192.1.1.103	10.2.2.200	TCP	54	25 → 17622 [RST, ACK] Seq=1 Ack=1 Win

```
PC3> ping 192.1.1.103 -P 6 -p 25
Connect   25@192.1.1.103 RST returned
Connect   25@192.1.1.103 RST returned
Connect   25@192.1.1.103 RST returned
Connect   25@192.1.1.103 RST returned
Connect   25@192.1.1.103 RST returned
```

Figura 2.5: Ping TCP do PC3 (professor) para EMAIL na DMZ com sucesso. Pacotes capturados entre PC3 e Switch4

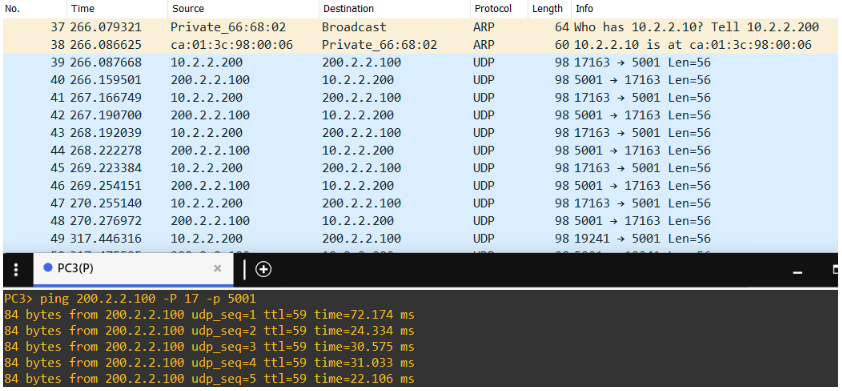
2.4.2 FROM-INSIDE-TO-OUTSIDE

2.4.2.1 Configuração

Para as comunicações originadas em INSIDE com destino a OUTSIDE (internet), permitimos o tráfego de pacotes UDP na gama de portas de destino 5000-6000:

```
set firewall name FROM-INSIDE-TO-OUTSIDE rule 10 action 'accept'
set firewall name FROM-INSIDE-TO-OUTSIDE rule 10 destination port '5000-6000'
set firewall name FROM-INSIDE-TO-OUTSIDE rule 10 protocol 'udp'
```

2.4.2.2 Teste



```
No.   Time          Source              Destination         Protocol  Length  Info
  37 266.079321    Private_66:68:02    Broadcast           ARP           64  Who has 10.2.2.10? Tell 10.2.2.200
  38 266.086625    ca:01:3c:98:00:06   Private_66:68:02    ARP           60  10.2.2.10 is at ca:01:3c:98:00:06
  39 266.087668    10.2.2.200          200.2.2.100         UDP           98  17163 → 5001 Len=56
  40 266.159501    200.2.2.100         10.2.2.200          UDP           98  5001 → 17163 Len=56
  41 267.166749    10.2.2.200          200.2.2.100         UDP           98  17163 → 5001 Len=56
  42 267.190700    200.2.2.100         10.2.2.200          UDP           98  5001 → 17163 Len=56
  43 268.192039    10.2.2.200          200.2.2.100         UDP           98  17163 → 5001 Len=56
  44 268.222278    200.2.2.100         10.2.2.200          UDP           98  5001 → 17163 Len=56
  45 269.223384    10.2.2.200          200.2.2.100         UDP           98  17163 → 5001 Len=56
  46 269.254151    200.2.2.100         10.2.2.200          UDP           98  5001 → 17163 Len=56
  47 270.255140    10.2.2.200          200.2.2.100         UDP           98  17163 → 5001 Len=56
  48 270.276972    200.2.2.100         10.2.2.200          UDP           98  5001 → 17163 Len=56
  49 317.446316    10.2.2.200          200.2.2.100         UDP           98  19241 → 5001 Len=56
```

```
PC3> ping 200.2.2.100 -P 17 -p 5001
84 bytes from 200.2.2.100 udp_seq=1 ttl=59 time=72.174 ms
84 bytes from 200.2.2.100 udp_seq=2 ttl=59 time=24.334 ms
84 bytes from 200.2.2.100 udp_seq=3 ttl=59 time=30.575 ms
84 bytes from 200.2.2.100 udp_seq=4 ttl=59 time=31.033 ms
84 bytes from 200.2.2.100 udp_seq=5 ttl=59 time=22.106 ms
```

Figura 2.6: Ping UDP do PC3 (professor) para 200.2.2.100 na zona OUTSIDE com sucesso. Pacotes capturados entre PC3 e Switch4

2.4.3 FROM-OUTSIDE-TO-INSIDE

2.4.3.1 Configuração

Esta regra indica que a firewall permite conexões estabelecidas e relacionadas na direção **OUTSIDE** a **INSIDE**.

```
set firewall name FROM-OUTSIDE-TO-INSIDE rule 10 action accept
set firewall name FROM-OUTSIDE-TO-INSIDE rule 10 description "Accept
Established-Related Connections"
set firewall name FROM-OUTSIDE-TO-INSIDE rule 10 state established enable
set firewall name FROM-OUTSIDE-TO-INSIDE rule 10 state related enable
```

2.4.4 FROM-DMZ-TO-INSIDE

2.4.4.1 Configuração

Assim como na regra 2.4.3, para esta seguimos o mesmo princípio em que aceitamos conexões estabelecidas e relacionadas só que neste caso é na direção **DMZ** a **INSIDE**.

```
set firewall name FROM-DMZ-TO-INSIDE rule 10 action ’accept’
set firewall name FROM-DMZ-TO-INSIDE rule 10 state established ’enable’
set firewall name FROM-DMZ-TO-INSIDE rule 10 state related ’enable’
```

Load-Balancers Deployment

Configuramos os load balancers VyOS com alta disponibilidade usando o Protocolo de Redundância de Roteador Virtual (VRRP) na interface eth1 e também habilitamos o balanceamento de carga na WAN. Além disso, são configuradas funcionalidades de sincronização de estado de conexão (conntrack-sync). A seguir vamos exemplificar a configuração dos diversos protocolos em um load balancer. A configuração nos restantes load balancers é análoga a esta:

3.1 Rotas estáticas

Para os LB1A e LB1B fizemos esta rota estática para encaminhar os pacotes ara o **INSIDE**:

```
set protocols static route 10.2.2.0/24 next-hop 10.1.1.10
```

Para o LB2A e o LB2B para encaminhar o trafego para o **OUTSIDE**:

```
set protocols static route 200.2.2.0/24 next-hop 200.1.1.10
```

3.2 VRRP

3.2.1 Configuração

No VRRP, dois load balancers são configurados para formar um grupo de routers virtuais para garantir disponibilidade de seus serviços.

```
set high-availability vrrp group LB1Cluster interface ’eth1’
set high-availability vrrp group LB1Cluster rfc3768-compatibility
set high-availability vrrp group LB1Cluster virtual-address ’30.0.0.5/30’
set high-availability vrrp group LB1Cluster vrid ’1’
set high-availability vrrp sync-group LB1Cluster member ’LB1Cluster’
```

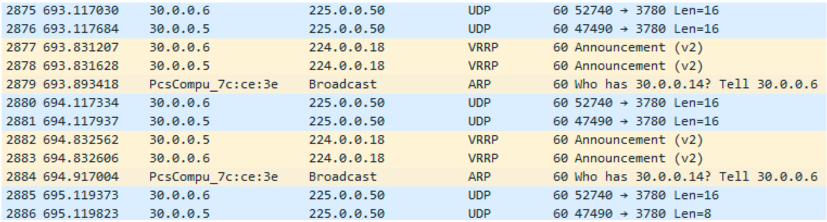
3.3 Conntrack-sync:

3.3.1 Configuração

O conntrack-sync sincroniza as conexões de rede entre dois load balancers para garantir alta disponibilidade e failover suave, evitando interrupções ou perda de conexão em caso de falha de um dos load balancers. Ele replica o estado das conexões ativas entre os dois dispositivos, permitindo que o tráfego seja redirecionado sem problemas em caso de falha.

```
set service conntrack-sync accept-protocol 'tcp,udp,icmp'
set service conntrack-sync disable-external-cache
set service conntrack-sync event-listen-queue-size '8'
set service conntrack-sync failover-mechanism vrrp sync-group 'LB1Cluster'
set service conntrack-sync interface eth1
set service conntrack-sync mcast-group '225.0.0.50'
set service conntrack-sync sync-queue-size '1'
```

3.3.2 Teste:



```
2875 693.117030   30.0.0.6          225.0.0.50    UDP     60 52740 → 3780 Len=16
2876 693.117684   30.0.0.5          225.0.0.50    UDP     60 47490 → 3780 Len=16
2877 693.831207   30.0.0.6          224.0.0.18    VRRP    60 Announcement (v2)
2878 693.831628   30.0.0.5          224.0.0.18    VRRP    60 Announcement (v2)
2879 693.893418   PcsCompu_7c:ce:3e Broadcast     ARP     60 Who has 30.0.0.14? Tell 30.0.0.6
2880 694.117334   30.0.0.6          225.0.0.50    UDP     60 52740 → 3780 Len=16
2881 694.117937   30.0.0.5          225.0.0.50    UDP     60 47490 → 3780 Len=16
2882 694.832562   30.0.0.5          224.0.0.18    VRRP    60 Announcement (v2)
2883 694.832606   30.0.0.6          224.0.0.18    VRRP    60 Announcement (v2)
2884 694.917004   PcsCompu_7c:ce:3e Broadcast     ARP     60 Who has 30.0.0.14? Tell 30.0.0.6
2885 695.119373   30.0.0.6          225.0.0.50    UDP     60 52740 → 3780 Len=16
2886 695.119823   30.0.0.5          225.0.0.50    UDP     60 47490 → 3780 Len=8
```

Figura 3.1: Captura entre o LB1A e o LB1B

3.4 Load-balancing:

3.4.1 Configuração

O objetivo aqui é distribuir o tráfego de saída de forma equilibrada entre as interfaces especificadas, monitorando sua integridade para garantir a eficiência e a disponibilidade do sistema.

```
set load-balancing wan disable-source-nat
set load-balancing wan interface-health eth0 failure-count '1'
set load-balancing wan interface-health eth0 nexthop '30.0.0.2'
set load-balancing wan interface-health eth0 success-count '1'
set load-balancing wan interface-health eth2 failure-count '1'
set load-balancing wan interface-health eth2 nexthop '30.0.0.18'
set load-balancing wan interface-health eth2 success-count '1'
set load-balancing wan rule 1 inbound-interface ’eth3’
set load-balancing wan rule 1 interface eth0 weight ’1’
set load-balancing wan rule 1 interface eth2 weight ’1’
set load-balancing wan rule 1 protocol ’all’
set load-balancing wan sticky-connections inbound
```

Appendix - full commands

```
# LB1A ----------------------------------
set high-availability vrrp group LB1Cluster interface ’eth1’
set high-availability vrrp group LB1Cluster rfc3768-compatibility
set high-availability vrrp group LB1Cluster virtual-address ’30.0.0.5/30’
set high-availability vrrp group LB1Cluster vrid ’1’
set high-availability vrrp sync-group LB1Cluster member ’LB1Cluster’
set interfaces ethernet eth0 address ’30.0.0.1/30’
set interfaces ethernet eth0 duplex ’auto’
set interfaces ethernet eth0 hw-id ’08:00:27:a1:71:12’
set interfaces ethernet eth0 smp-affinity ’auto’
set interfaces ethernet eth0 speed ’auto’
set interfaces ethernet eth1 address ’30.0.0.5/30’
set interfaces ethernet eth1 duplex ’auto’
set interfaces ethernet eth1 hw-id ’08:00:27:e3:65:10’
set interfaces ethernet eth1 smp-affinity ’auto’
set interfaces ethernet eth1 speed ’auto’
set interfaces ethernet eth2 address ’30.0.0.17/30’
set interfaces ethernet eth2 duplex ’auto’
set interfaces ethernet eth2 hw-id ’08:00:27:e4:b6:e3’
set interfaces ethernet eth2 smp-affinity ’auto’
set interfaces ethernet eth2 speed ’auto’
set interfaces ethernet eth3 address ’10.1.1.11/24’
set interfaces ethernet eth3 duplex ’auto’
set interfaces ethernet eth3 hw-id ’08:00:27:c2:21:7c’
set interfaces ethernet eth3 smp-affinity ’auto’
set interfaces ethernet eth3 speed ’auto’
set interfaces loopback lo
set load-balancing wan disable-source-nat
set load-balancing wan interface-health eth0 failure-count ’1’
set load-balancing wan interface-health eth0 nexthop ’30.0.0.2’
set load-balancing wan interface-health eth0 success-count ’1’
set load-balancing wan interface-health eth2 failure-count ’1’
set load-balancing wan interface-health eth2 nexthop ’30.0.0.18’
set load-balancing wan interface-health eth2 success-count '1'
set load-balancing wan rule 1 inbound-interface 'eth3'
set load-balancing wan rule 1 interface eth0 weight '1'
set load-balancing wan rule 1 interface eth2 weight '1'
set load-balancing wan rule 1 protocol 'all'
set load-balancing wan sticky-connections inbound
set protocols static route 10.2.2.0/24 next-hop 10.1.1.10
set service conntrack-sync accept-protocol 'tcp,udp,icmp'
set service conntrack-sync disable-external-cache
set service conntrack-sync event-listen-queue-size '8'
set service conntrack-sync failover-mechanism vrrp sync-group 'LB1Cluster'
set service conntrack-sync interface eth1
set service conntrack-sync mcast-group '225.0.0.50'
set service conntrack-sync sync-queue-size '1'
set system config-management commit-revisions '100'
set system console device ttyS0 speed '9600'
set system host-name 'vyos'
set system login user vyos authentication encrypted-password '$6$QxPS.uk6mfo$9QBSo8u1FkH16gM
set system login user vyos authentication plaintext-password ''
set system login user vyos level 'admin'
set system ntp server 0.pool.ntp.org
set system ntp server 1.pool.ntp.org
set system ntp server 2.pool.ntp.org
set system syslog global facility all level 'info'
set system syslog global facility protocols level 'debug'
set system time-zone 'UTC'

#FW1 ---------------------------------
set firewall all-ping 'enable'
set firewall broadcast-ping 'disable'
set firewall config-trap 'disable'
set firewall ipv6-receive-redirects 'disable'
set firewall ipv6-src-route 'disable'
set firewall ip-src-route 'disable'
set firewall log-martians 'enable'
set firewall name FROM-DMZ-TO-INSIDE default-action 'drop'
set firewall name FROM-DMZ-TO-INSIDE rule 10 action 'accept'
set firewall name FROM-DMZ-TO-INSIDE rule 10 state established 'enable'
set firewall name FROM-DMZ-TO-INSIDE rule 10 state related 'enable'
set firewall name FROM-INSIDE-TO-DMZ default-action 'drop'
set firewall name FROM-INSIDE-TO-DMZ rule 10 action 'accept'
set firewall name FROM-INSIDE-TO-DMZ rule 10 destination address '192.1.1.100'
set firewall name FROM-INSIDE-TO-DMZ rule 10 destination port '80'
set firewall name FROM-INSIDE-TO-DMZ rule 10 limit burst '1'
set firewall name FROM-INSIDE-TO-DMZ rule 10 protocol 'tcp'
set firewall name FROM-INSIDE-TO-DMZ rule 20 action 'accept'
set firewall name FROM-INSIDE-TO-DMZ rule 20 destination port ’443’
set firewall name FROM-INSIDE-TO-DMZ rule 20 protocol ’tcp’
set firewall name FROM-INSIDE-TO-DMZ rule 30 action ’accept’
set firewall name FROM-INSIDE-TO-DMZ rule 30 destination port ’25’
set firewall name FROM-INSIDE-TO-DMZ rule 30 protocol ’tcp’
set firewall name FROM-INSIDE-TO-DMZ rule 40 action ’accept’
set firewall name FROM-INSIDE-TO-DMZ rule 40 destination address ’192.1.1.103’
set firewall name FROM-INSIDE-TO-DMZ rule 40 destination port ’22’
set firewall name FROM-INSIDE-TO-DMZ rule 40 protocol ’tcp’
set firewall name FROM-INSIDE-TO-DMZ rule 40 source address ’10.2.2.200-10.2.2.254’
set firewall name FROM-INSIDE-TO-DMZ rule 60 action ’drop’
set firewall name FROM-INSIDE-TO-DMZ rule 60 limit burst ’1’
set firewall name FROM-INSIDE-TO-DMZ rule 60 limit rate ’5/second’
set firewall name FROM-INSIDE-TO-OUTSIDE default-action ’drop’
set firewall name FROM-INSIDE-TO-OUTSIDE rule 10 action ’accept’
set firewall name FROM-INSIDE-TO-OUTSIDE rule 10 destination port ’5000-6000’
set firewall name FROM-INSIDE-TO-OUTSIDE rule 10 protocol ’udp’
set firewall name FROM-OUTSIDE-TO-INSIDE default-action ’drop’
set firewall name FROM-OUTSIDE-TO-INSIDE rule 10 action ’accept’
set firewall name FROM-OUTSIDE-TO-INSIDE rule 10 state established ’enable’
set firewall receive-redirects ’disable’
set firewall send-redirects ’enable’
set firewall source-validation ’disable’
set firewall syn-cookies ’enable’
set firewall twa-hazards-protection ’disable’
set interfaces ethernet eth0 address ’30.0.0.2/30’
set interfaces ethernet eth0 duplex ’auto’
set interfaces ethernet eth0 hw-id ’08:00:27:7d:bc:10’
set interfaces ethernet eth0 smp-affinity ’auto’
set interfaces ethernet eth0 speed ’auto’
set interfaces ethernet eth1 address ’30.0.0.21/30’
set interfaces ethernet eth1 duplex ’auto’
set interfaces ethernet eth1 hw-id ’08:00:27:ec:34:d1’
set interfaces ethernet eth1 smp-affinity ’auto’
set interfaces ethernet eth1 speed ’auto’
set interfaces ethernet eth2 address ’30.0.0.14/30’
set interfaces ethernet eth2 duplex ’auto’
set interfaces ethernet eth2 hw-id ’08:00:27:48:c6:cb’
set interfaces ethernet eth2 smp-affinity ’auto’
set interfaces ethernet eth2 speed ’auto’
set interfaces ethernet eth3 address ’30.0.0.25/30’
set interfaces ethernet eth3 duplex ’auto’
set interfaces ethernet eth3 hw-id ’08:00:27:68:34:07’
set interfaces ethernet eth3 smp-affinity ’auto’
set interfaces ethernet eth3 speed ’auto’
set interfaces ethernet eth4 address ’192.1.1.101/24’
set interfaces ethernet eth4 duplex ’auto’
set interfaces ethernet eth4 hw-id ’08:00:27:bc:1d:aa’
set interfaces ethernet eth4 smp-affinity ’auto’
set interfaces ethernet eth4 speed ’auto’
set interfaces loopback lo
set nat source rule 100 outbound-interface ’eth1’
set nat source rule 100 source address ’10.2.2.0/24’
set nat source rule 100 translation address ’192.1.0.1-192.1.0.10’
set nat source rule 101 outbound-interface ’eth3’
set nat source rule 101 source address ’10.2.2.0/24’
set nat source rule 101 translation address ’192.1.0.11-192.1.0.20’
set protocols static route 10.2.2.0/24 next-hop 30.0.0.1
set protocols static route 10.2.2.0/24 next-hop 30.0.0.13
set protocols static route 200.2.2.0/24 next-hop 30.0.0.22
set protocols static route 200.2.2.0/24 next-hop 30.0.0.26
set system config-management commit-revisions ’100’
set system console device ttyS0 speed ’9600’
set system host-name ’vyos’
set system login user vyos authentication encrypted-password ’$6$QxPS.uk6mfo$9QBSo8u1FkH16gM
set system login user vyos authentication plaintext-password ’’
set system login user vyos level ’admin’
set system ntp server 0.pool.ntp.org
set system ntp server 1.pool.ntp.org
set system ntp server 2.pool.ntp.org
set system syslog global facility all level ’info’
set system syslog global facility protocols level ’debug’
set system time-zone ’UTC’
set zone-policy zone DMZ default-action ’drop’
set zone-policy zone DMZ description ’Dmz’
set zone-policy zone DMZ from INSIDE firewall name ’FROM-INSIDE-TO-DMZ’
set zone-policy zone DMZ interface ’eth4’
set zone-policy zone INSIDE default-action ’drop’
set zone-policy zone INSIDE description ’Inside’
set zone-policy zone INSIDE from DMZ firewall name ’FROM-DMZ-TO-INSIDE’
set zone-policy zone INSIDE from OUTSIDE firewall name ’FROM-OUTSIDE-TO-INSIDE’
set zone-policy zone INSIDE interface ’eth0’
set zone-policy zone INSIDE interface ’eth2’
set zone-policy zone OUTSIDE default-action ’drop’
set zone-policy zone OUTSIDE description ’Outside’
set zone-policy zone OUTSIDE from INSIDE firewall name ’FROM-INSIDE-TO-OUTSIDE’
set zone-policy zone OUTSIDE interface ’eth1’
set zone-policy zone OUTSIDE interface ’eth3’

#FW2 ---------------------------------
set firewall all-ping ’enable’
set firewall broadcast-ping ’disable’
set firewall config-trap ’disable’
set firewall ipv6-receive-redirects ’disable’
set firewall ipv6-src-route ’disable’
set firewall ip-src-route ’disable’
set firewall log-martians ’enable’
set firewall name FROM-DMZ-TO-INSIDE default-action ’drop’
set firewall name FROM-DMZ-TO-INSIDE rule 10 action ’accept’
set firewall name FROM-DMZ-TO-INSIDE rule 10 state established ’enable’
set firewall name FROM-DMZ-TO-INSIDE rule 10 state related ’enable’
set firewall name FROM-INSIDE-TO-DMZ default-action ’drop’
set firewall name FROM-INSIDE-TO-DMZ rule 10 action ’accept’
set firewall name FROM-INSIDE-TO-DMZ rule 10 destination address ’192.1.1.100’
set firewall name FROM-INSIDE-TO-DMZ rule 10 destination port ’80’
set firewall name FROM-INSIDE-TO-DMZ rule 10 protocol ’tcp’
set firewall name FROM-INSIDE-TO-DMZ rule 20 action ’accept’
set firewall name FROM-INSIDE-TO-DMZ rule 20 destination port ’443’
set firewall name FROM-INSIDE-TO-DMZ rule 20 protocol ’tcp’
set firewall name FROM-INSIDE-TO-DMZ rule 30 action ’accept’
set firewall name FROM-INSIDE-TO-DMZ rule 30 destination port ’25’
set firewall name FROM-INSIDE-TO-DMZ rule 30 protocol ’tcp’
set firewall name FROM-INSIDE-TO-DMZ rule 40 action ’accept’
set firewall name FROM-INSIDE-TO-DMZ rule 40 destination address ’192.1.1.103’
set firewall name FROM-INSIDE-TO-DMZ rule 40 destination port ’22’
set firewall name FROM-INSIDE-TO-DMZ rule 40 protocol ’tcp’
set firewall name FROM-INSIDE-TO-DMZ rule 40 source address ’10.2.2.200-10.2.2.254’
set firewall name FROM-INSIDE-TO-DMZ rule 60 action ’drop’
set firewall name FROM-INSIDE-TO-DMZ rule 60 limit burst ’1’
set firewall name FROM-INSIDE-TO-DMZ rule 60 limit rate ’5/second’
set firewall name FROM-INSIDE-TO-OUTSIDE default-action ’drop’
set firewall name FROM-INSIDE-TO-OUTSIDE rule 10 action ’accept’
set firewall name FROM-INSIDE-TO-OUTSIDE rule 10 destination port ’5000-6000’
set firewall name FROM-INSIDE-TO-OUTSIDE rule 10 protocol ’udp’
set firewall name FROM-OUTSIDE-TO-INSIDE default-action ’drop’
set firewall name FROM-OUTSIDE-TO-INSIDE rule 10 action ’accept’
set firewall name FROM-OUTSIDE-TO-INSIDE rule 10 state established ’enable’
set firewall receive-redirects ’disable’
set firewall send-redirects ’enable’
set firewall source-validation ’disable’
set firewall syn-cookies ’enable’
set firewall twa-hazards-protection ’disable’
set interfaces ethernet eth0 address ’30.0.0.10/30’
set interfaces ethernet eth0 duplex ’auto’
set interfaces ethernet eth0 hw-id ’08:00:27:2b:17:90’
set interfaces ethernet eth0 smp-affinity ’auto’
set interfaces ethernet eth0 speed ’auto’
set interfaces ethernet eth1 address ’30.0.0.18/30’
set interfaces ethernet eth1 duplex 'auto'
set interfaces ethernet eth1 hw-id '08:00:27:05:d8:39'
set interfaces ethernet eth1 smp-affinity 'auto'
set interfaces ethernet eth1 speed 'auto'
set interfaces ethernet eth2 address '30.0.0.29/30'
set interfaces ethernet eth2 duplex 'auto'
set interfaces ethernet eth2 hw-id '08:00:27:c6:51:45'
set interfaces ethernet eth2 smp-affinity 'auto'
set interfaces ethernet eth2 speed 'auto'
set interfaces ethernet eth3 address '30.0.0.33/30'
set interfaces ethernet eth3 duplex 'auto'
set interfaces ethernet eth3 hw-id '08:00:27:44:e5:e8'
set interfaces ethernet eth3 smp-affinity 'auto'
set interfaces ethernet eth3 speed 'auto'
set interfaces ethernet eth4 address '192.1.1.102/24'
set interfaces ethernet eth4 duplex 'auto'
set interfaces ethernet eth4 hw-id '08:00:27:55:23:95'
set interfaces ethernet eth4 smp-affinity 'auto'
set interfaces ethernet eth4 speed 'auto'
set interfaces loopback lo
set nat source rule 100 outbound-interface 'eth2'
set nat source rule 100 source address '10.2.2.0/24'
set nat source rule 100 translation address '192.1.0.21-192.1.0.30'
set nat source rule 101 outbound-interface 'eth3'
set nat source rule 101 source address '10.2.2.0/24'
set nat source rule 101 translation address '192.1.0.31-192.1.0.40'
set protocols static route 10.2.2.0/24 next-hop 30.0.0.9
set protocols static route 10.2.2.0/24 next-hop 30.0.0.17
set protocols static route 200.2.2.0/24 next-hop 30.0.0.30
set protocols static route 200.2.2.0/24 next-hop 30.0.0.34
set system config-management commit-revisions '100'
set system console device ttyS0 speed '9600'
set system host-name 'vyos'
set system login user vyos authentication encrypted-password '$6$QxPS.uk6mfo$9QBSo8u1FkH16gM
set system login user vyos authentication plaintext-password ''
set system login user vyos level 'admin'
set system ntp server 0.pool.ntp.org
set system ntp server 1.pool.ntp.org
set system ntp server 2.pool.ntp.org
set system syslog global facility all level 'info'
set system syslog global facility protocols level 'debug'
set system time-zone 'UTC'
set zone-policy zone DMZ default-action 'drop'
set zone-policy zone DMZ description 'Dmz'
set zone-policy zone DMZ from INSIDE firewall name 'FROM-INSIDE-TO-DMZ'
set zone-policy zone DMZ interface 'eth4'
set zone-policy zone INSIDE default-action 'drop'
set zone-policy zone INSIDE description 'Inside'
set zone-policy zone INSIDE from DMZ firewall name 'FROM-DMZ-TO-INSIDE'
set zone-policy zone INSIDE from OUTSIDE firewall name 'FROM-OUTSIDE-TO-INSIDE'
set zone-policy zone INSIDE interface 'eth0'
set zone-policy zone INSIDE interface 'eth1'
set zone-policy zone OUTSIDE default-action 'drop'
set zone-policy zone OUTSIDE description 'Outside'
set zone-policy zone OUTSIDE from INSIDE firewall name 'FROM-INSIDE-TO-OUTSIDE'
set zone-policy zone OUTSIDE interface 'eth2'
set zone-policy zone OUTSIDE interface 'eth3'

#LB1B ---------------------------------
set high-availability vrrp group LB1Cluster interface 'eth1'
set high-availability vrrp group LB1Cluster rfc3768-compatibility
set high-availability vrrp group LB1Cluster virtual-address '30.0.0.6/30'
set high-availability vrrp group LB1Cluster vrid '1'
set high-availability vrrp sync-group LB1Cluster member 'LB1Cluster'
set interfaces ethernet eth0 address '30.0.0.13/30'
set interfaces ethernet eth0 duplex 'auto'
set interfaces ethernet eth0 hw-id '08:00:27:ed:ec:3a'
set interfaces ethernet eth0 smp-affinity 'auto'
set interfaces ethernet eth0 speed 'auto'
set interfaces ethernet eth1 address '30.0.0.6/30'
set interfaces ethernet eth1 duplex 'auto'
set interfaces ethernet eth1 hw-id '08:00:27:03:40:1c'
set interfaces ethernet eth1 smp-affinity 'auto'
set interfaces ethernet eth1 speed 'auto'
set interfaces ethernet eth2 address '30.0.0.9/30'
set interfaces ethernet eth2 duplex 'auto'
set interfaces ethernet eth2 hw-id '08:00:27:a2:ee:f2'
set interfaces ethernet eth2 smp-affinity 'auto'
set interfaces ethernet eth2 speed 'auto'
set interfaces ethernet eth3 address '10.1.1.12/24'
set interfaces ethernet eth3 duplex 'auto'
set interfaces ethernet eth3 hw-id '08:00:27:72:ee:a3'
set interfaces ethernet eth3 smp-affinity 'auto'
set interfaces ethernet eth3 speed 'auto'
set interfaces loopback lo
set load-balancing wan disable-source-nat
set load-balancing wan interface-health eth0 failure-count '1'
set load-balancing wan interface-health eth0 nexthop '30.0.0.14'
set load-balancing wan interface-health eth0 success-count '1'
set load-balancing wan interface-health eth2 failure-count '1'
set load-balancing wan interface-health eth2 nexthop '30.0.0.10'
set load-balancing wan interface-health eth2 success-count '1'
set load-balancing wan rule 1 inbound-interface 'eth3'
set load-balancing wan rule 1 interface eth0 weight '1'
set load-balancing wan rule 1 interface eth2 weight '1'
set load-balancing wan rule 1 protocol 'all'
set load-balancing wan sticky-connections inbound
set protocols static route 10.2.2.0/24 next-hop 10.1.1.10
set service conntrack-sync accept-protocol 'tcp,udp,icmp'
set service conntrack-sync disable-external-cache
set service conntrack-sync event-listen-queue-size '8'
set service conntrack-sync failover-mechanism vrrp sync-group 'LB1Cluster'
set service conntrack-sync interface eth1
set service conntrack-sync mcast-group '225.0.0.50'
set service conntrack-sync sync-queue-size '1'
set system config-management commit-revisions '100'
set system console device ttyS0 speed '9600'
set system host-name 'vyos'
set system login user vyos authentication encrypted-password '$6$QxPS.uk6mfo$9QBSo8u1FkH16gM
set system login user vyos authentication plaintext-password ''
set system login user vyos level 'admin'
set system ntp server 0.pool.ntp.org
set system ntp server 1.pool.ntp.org
set system ntp server 2.pool.ntp.org
set system syslog global facility all level 'info'
set system syslog global facility protocols level 'debug'
set system time-zone 'UTC'

#LB2A ----------------------------------
set high-availability vrrp group LB2Cluster interface 'eth1'
set high-availability vrrp group LB2Cluster rfc3768-compatibility
set high-availability vrrp group LB2Cluster virtual-address '30.0.0.37/30'
set high-availability vrrp group LB2Cluster vrid '11'
set high-availability vrrp sync-group LB2Cluster member 'LB2Cluster'
set interfaces ethernet eth0 address '30.0.0.22/30'
set interfaces ethernet eth0 duplex 'auto'
set interfaces ethernet eth0 hw-id '08:00:27:45:8a:1a'
set interfaces ethernet eth0 smp-affinity 'auto'
set interfaces ethernet eth0 speed 'auto'
set interfaces ethernet eth1 address '30.0.0.37/30'
set interfaces ethernet eth1 duplex 'auto'
set interfaces ethernet eth1 hw-id '08:00:27:7b:a2:2b'
set interfaces ethernet eth1 smp-affinity 'auto'
set interfaces ethernet eth1 speed 'auto'
set interfaces ethernet eth2 address '30.0.0.34/30'
set interfaces ethernet eth2 duplex 'auto'
set interfaces ethernet eth2 hw-id '08:00:27:e1:d5:dc'
set interfaces ethernet eth2 smp-affinity 'auto'
set interfaces ethernet eth2 speed 'auto'
set interfaces ethernet eth3 address '200.1.1.11/24'
set interfaces ethernet eth3 duplex 'auto'
set interfaces ethernet eth3 hw-id '08:00:27:f8:e7:d3'
set interfaces ethernet eth3 smp-affinity 'auto'
set interfaces ethernet eth3 speed 'auto'
set interfaces loopback lo
set load-balancing wan disable-source-nat
set load-balancing wan interface-health eth0 failure-count '1'
set load-balancing wan interface-health eth0 nexthop '30.0.0.21'
set load-balancing wan interface-health eth0 success-count '1'
set load-balancing wan interface-health eth2 failure-count '1'
set load-balancing wan interface-health eth2 nexthop '30.0.0.29'
set load-balancing wan interface-health eth2 success-count '1'
set load-balancing wan rule 1 inbound-interface 'eth3'
set load-balancing wan rule 1 interface eth0 weight '1'
set load-balancing wan rule 1 interface eth2 weight '1'
set load-balancing wan rule 1 protocol 'all'
set load-balancing wan sticky-connections inbound
set protocols static route 200.2.2.0/24 next-hop 200.1.1.10
set service conntrack-sync accept-protocol 'tcp,udp,icmp'
set service conntrack-sync disable-external-cache
set service conntrack-sync event-listen-queue-size '8'
set service conntrack-sync failover-mechanism vrrp sync-group 'LB2Cluster'
set service conntrack-sync interface eth1
set service conntrack-sync mcast-group '225.0.0.0'
set service conntrack-sync sync-queue-size '1'
set system config-management commit-revisions '100'
set system console device ttyS0 speed '9600'
set system host-name 'vyos'
set system login user vyos authentication encrypted-password '$6$QxPS.uk6mfo$9QBSo8u1FkH16gM
set system login user vyos authentication plaintext-password ''
set system login user vyos level 'admin'
set system ntp server 0.pool.ntp.org
set system ntp server 1.pool.ntp.org
set system ntp server 2.pool.ntp.org
set system syslog global facility all level 'info'
set system syslog global facility protocols level 'debug'
set system time-zone 'UTC'

#LB2B ---------------------------------
set high-availability vrrp group LB2Cluster interface 'eth1'
set high-availability vrrp group LB2Cluster rfc3768-compatibility
set high-availability vrrp group LB2Cluster virtual-address '30.0.0.38/30'
set high-availability vrrp group LB2Cluster vrid '11'
set high-availability vrrp sync-group LB2Cluster member 'LB2Cluster'
set interfaces ethernet eth0 address ’30.0.0.26/30’
set interfaces ethernet eth0 duplex ’auto’
set interfaces ethernet eth0 hw-id ’08:00:27:cd:11:bc’
set interfaces ethernet eth3 duplex ’auto’
set interfaces ethernet eth3 hw-id ’08:00:27:5e:83:97’
set interfaces ethernet eth3 smp-affinity ’auto’
set interfaces ethernet eth3 speed ’auto’
set interfaces loopback lo
set load-balancing wan disable-source-nat
set load-balancing wan interface-health eth0 failure-count ’1’
set load-balancing wan interface-health eth0 nexthop ’30.0.0.25’
set load-balancing wan interface-health eth0 success-count ’1’
set load-balancing wan interface-health eth2 failure-count ’1’
set load-balancing wan interface-health eth2 nexthop ’30.0.0.29’
set load-balancing wan interface-health eth2 success-count ’1’
set load-balancing wan rule 1 inbound-interface ’eth3’
set load-balancing wan rule 1 interface eth0 weight ’1’
set load-balancing wan rule 1 interface eth2 weight ’1’
set load-balancing wan rule 1 protocol ’all’
set load-balancing wan sticky-connections inbound
set protocols static route 200.2.2.0/24 next-hop 200.1.1.10
set service conntrack-sync accept-protocol ’tcp,udp,icmp’
set service conntrack-sync disable-external-cache
set service conntrack-sync event-listen-queue-size ’8’
set service conntrack-sync failover-mechanism vrrp sync-group ’LB2Cluster’
set service conntrack-sync interface eth1
set service conntrack-sync mcast-group ’225.0.0.0’
set service conntrack-sync sync-queue-size ’1’
set system config-management commit-revisions ’100’
set system console device ttyS0 speed ’9600’
set system host-name ’vyos’
set system login user vyos authentication encrypted-password ’$6$QxPS.uk6mfo$9QBSo8u1FkH16gM
set system login user vyos authentication plaintext-password ’’
set system login user vyos level ’admin’
set system ntp server 0.pool.ntp.org
set system ntp server 1.pool.ntp.org
set system ntp server 2.pool.ntp.org
set system syslog global facility all level ’info’
set system syslog global facility protocols level ’debug’
set system time-zone ’UTC’
```