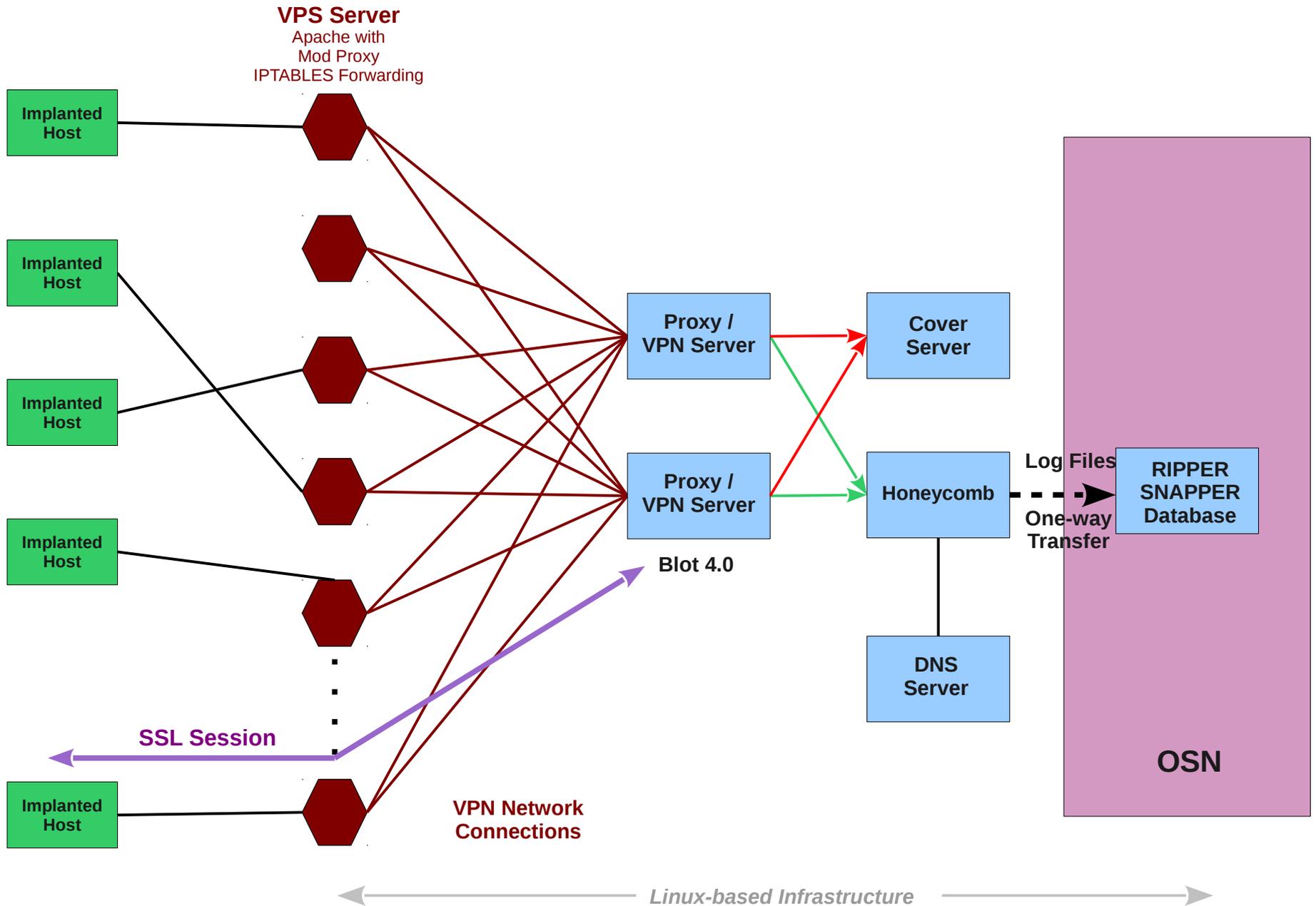
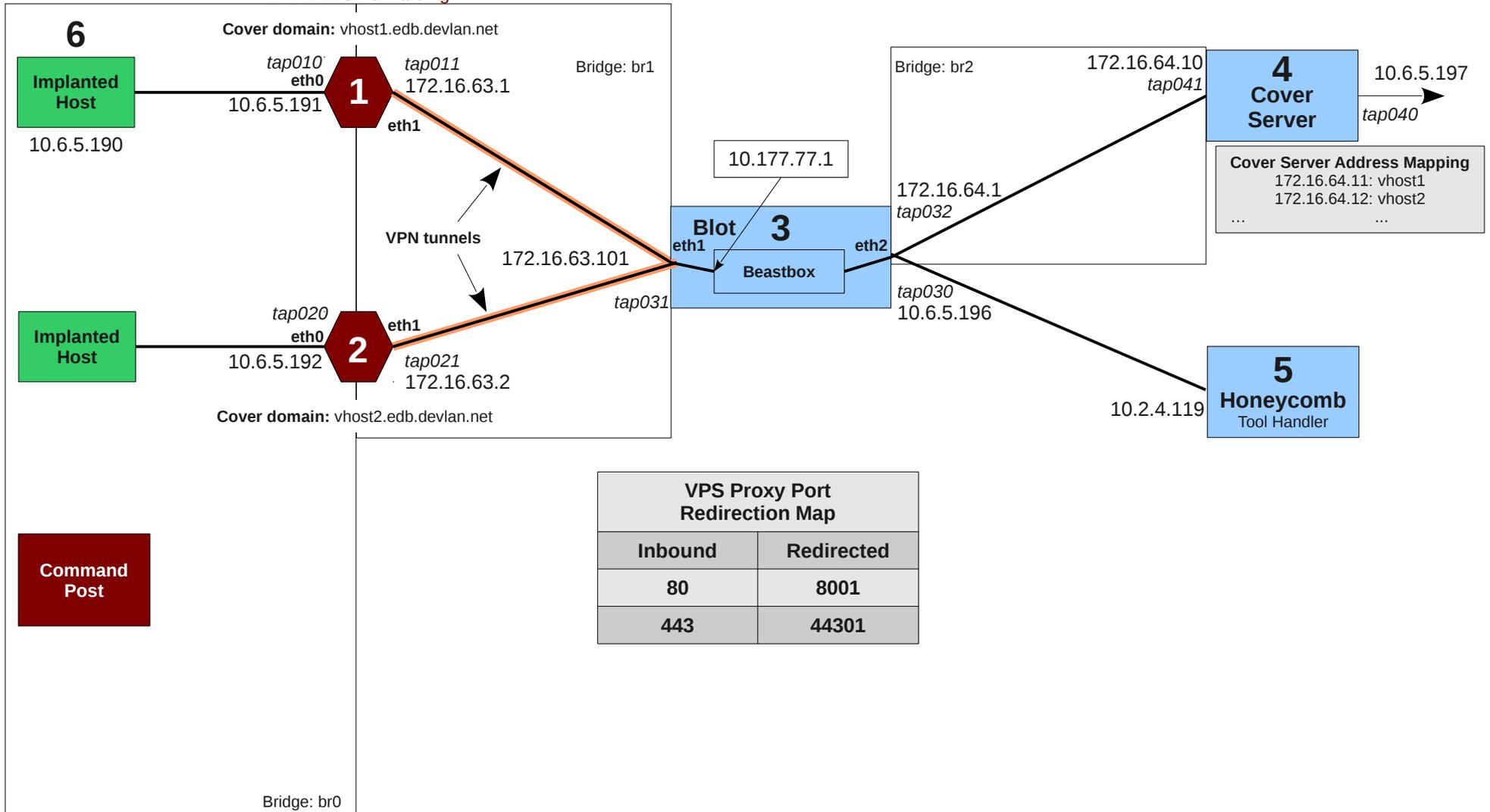


Hive Beacon Infrastructure

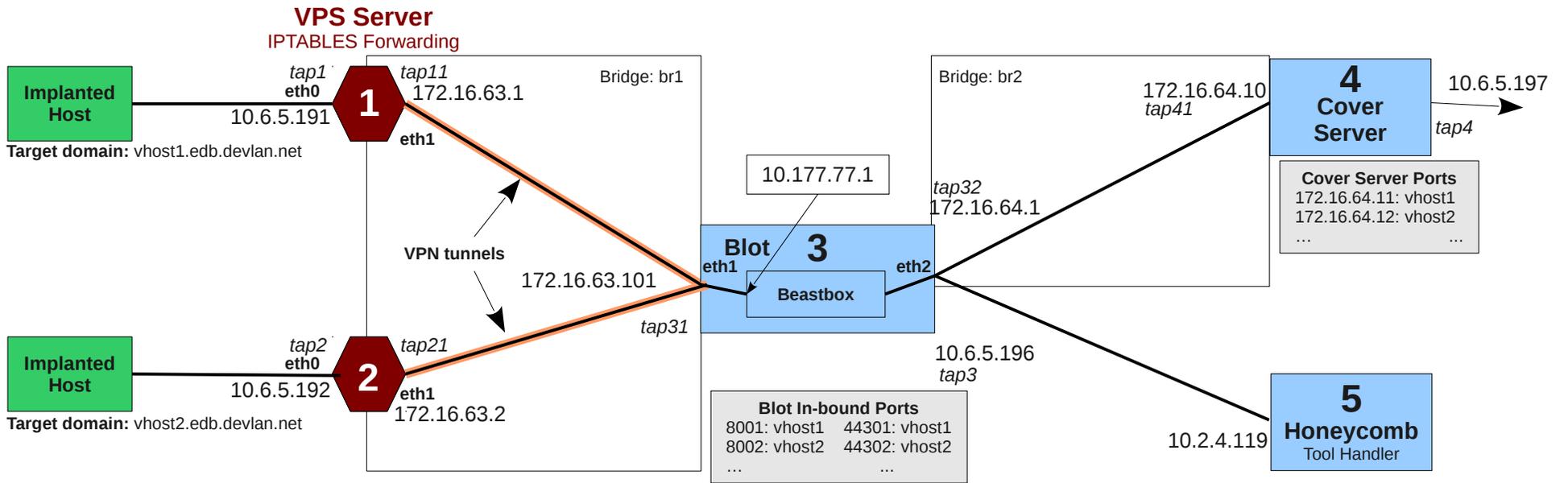


Hive Beacon Test Infrastructure

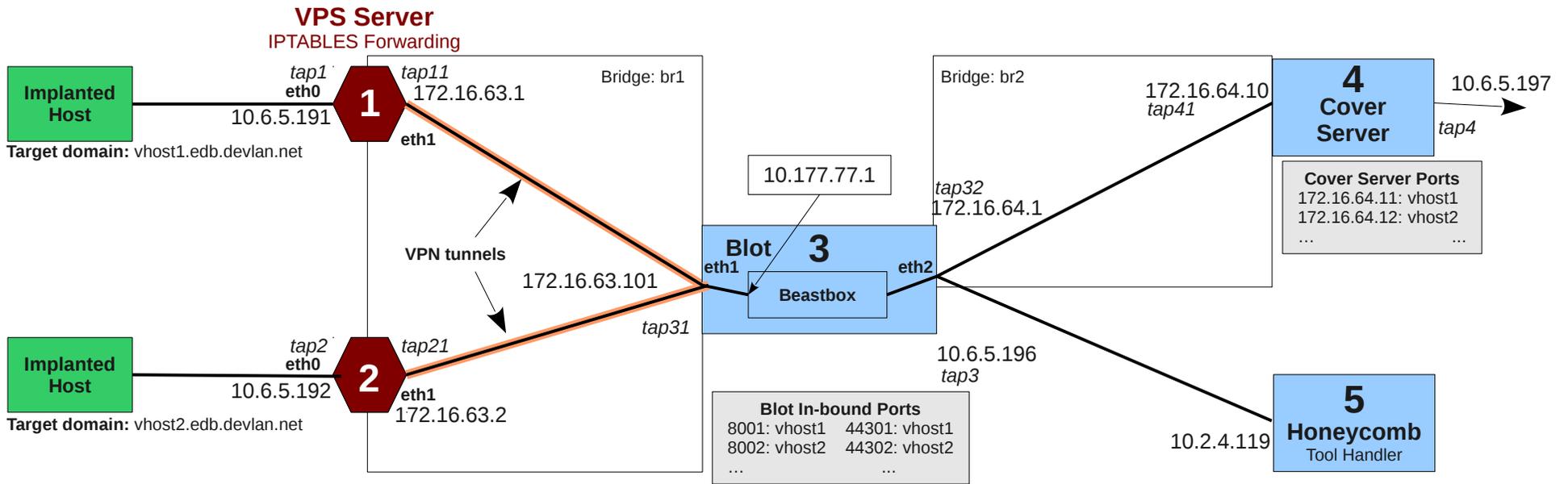
VPS Servers
IPTABLES Forwarding



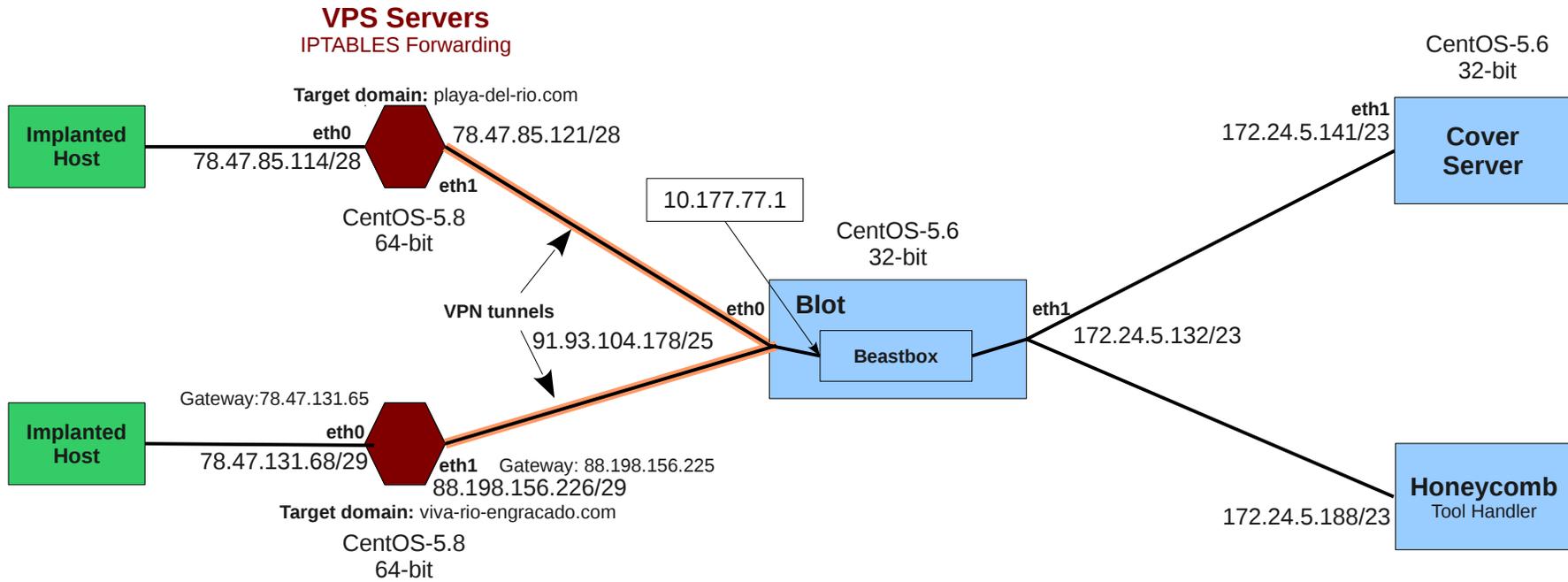
Hive Beacon Test Infrastructure



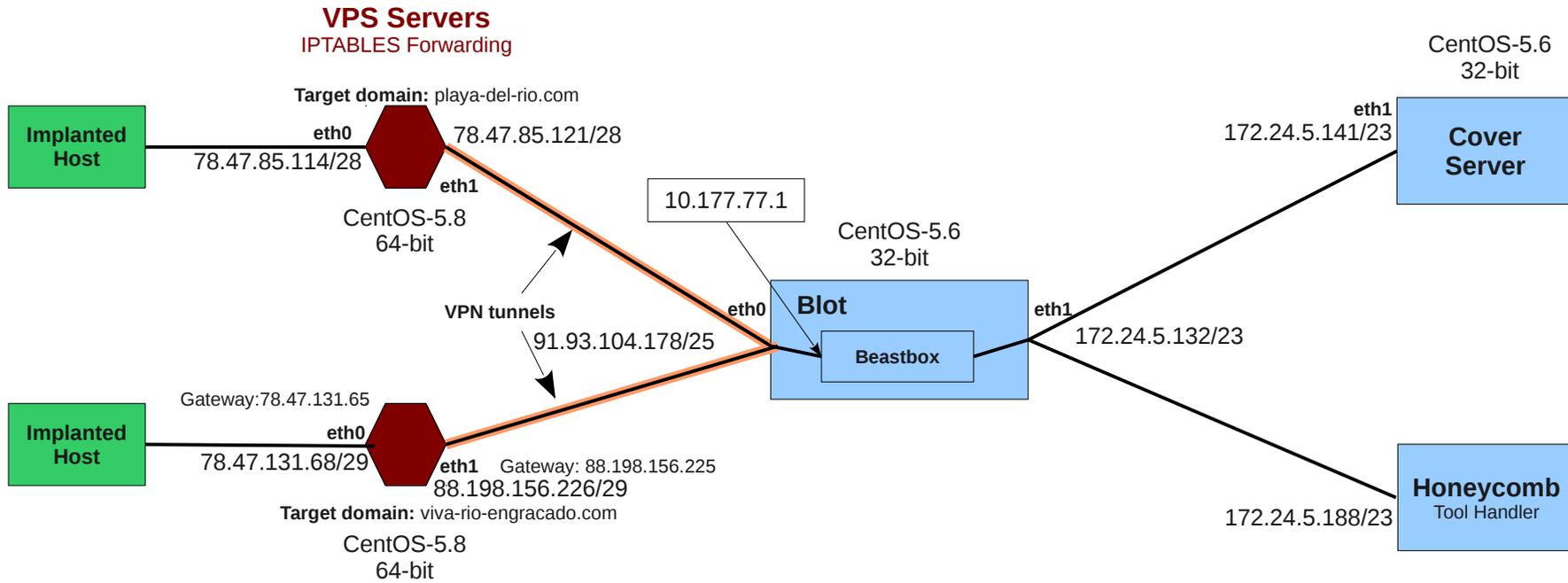
Hive Beacon Test Infrastructure



Hive Beacon Operational Infrastructure

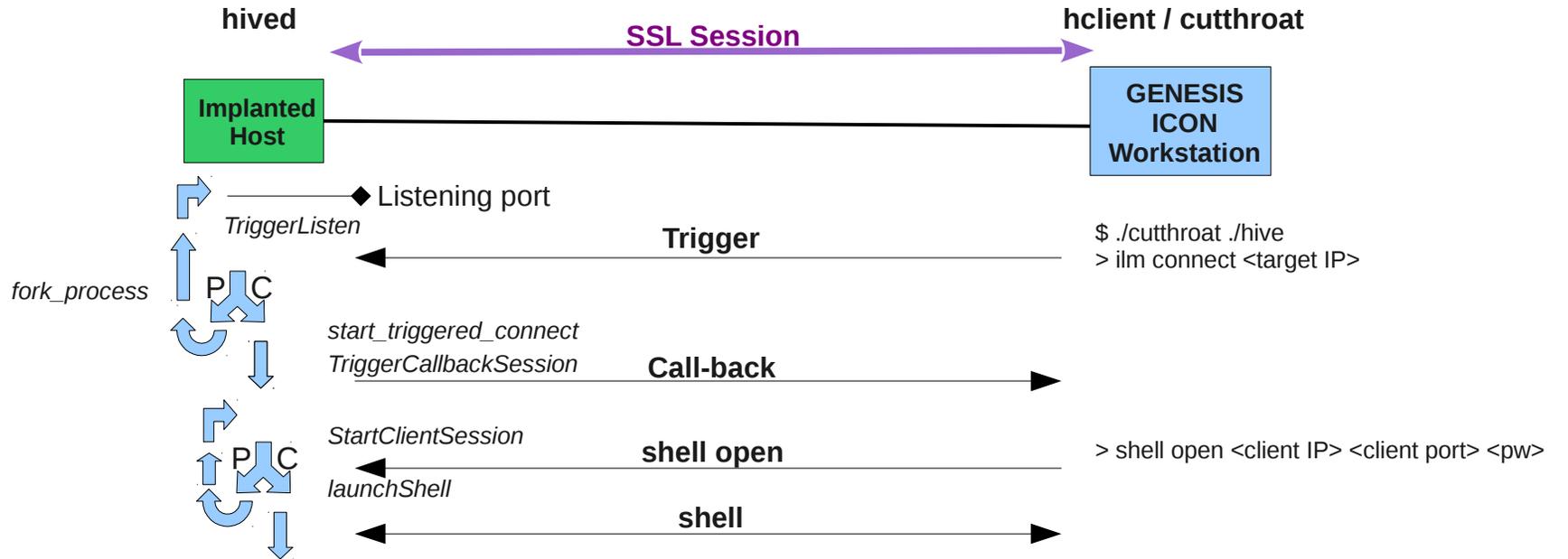


Hive Beacon Operational Infrastructure



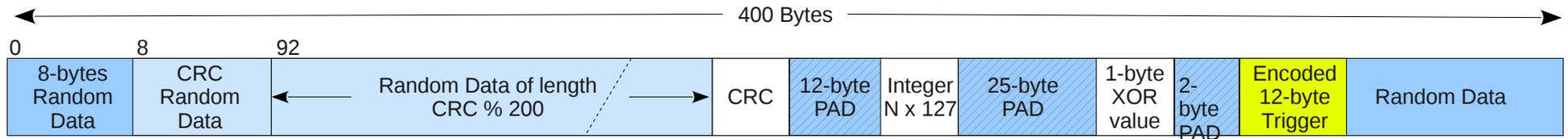
SinnerTwin Deployment Environment

Hive Operation



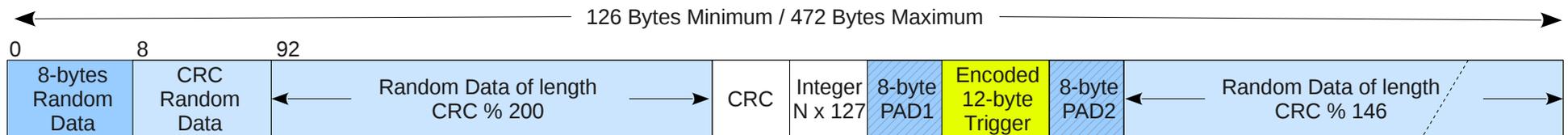
SECRET//NOFORN Raw TCP/UDP Trigger

Hive 2.5 Algorithm



The twelve byte trigger is encoded by XORing the 1-byte XOR value with the first five bytes of the trigger and the remaining trigger bytes or XORed with 0xB6.

Hive 2.6 Algorithm



The twelve byte trigger is encoded by computing an offset of CRC % 72 into the CRC random data field and XORing each of the twelve following bytes with the corresponding byte of the twelve-byte trigger payload.

Scrap slides follow

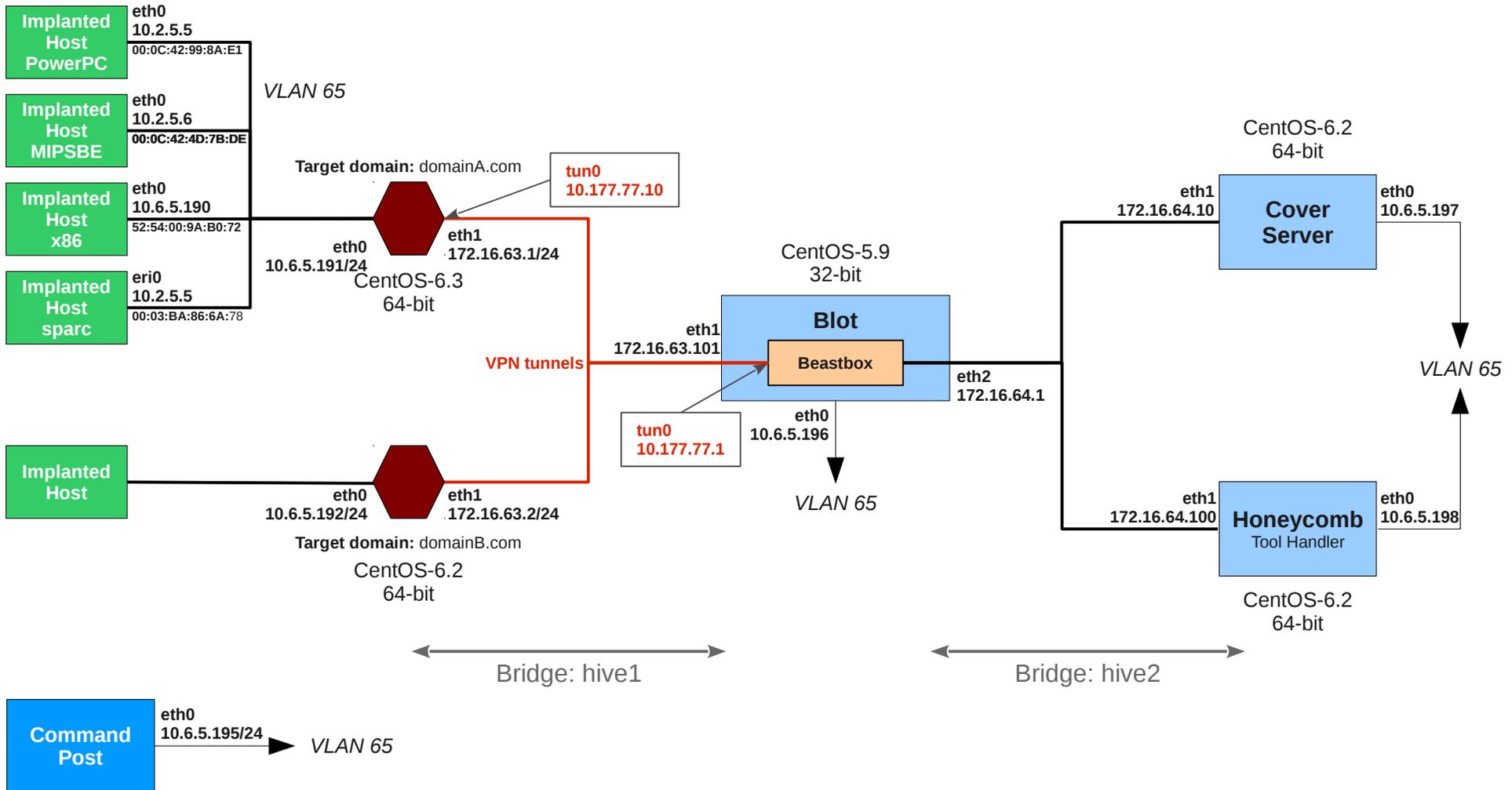
Hive Beacon Lab Test Infrastructure

Implanted Hosts

VPS Servers

Proxy / Director

Response Servers



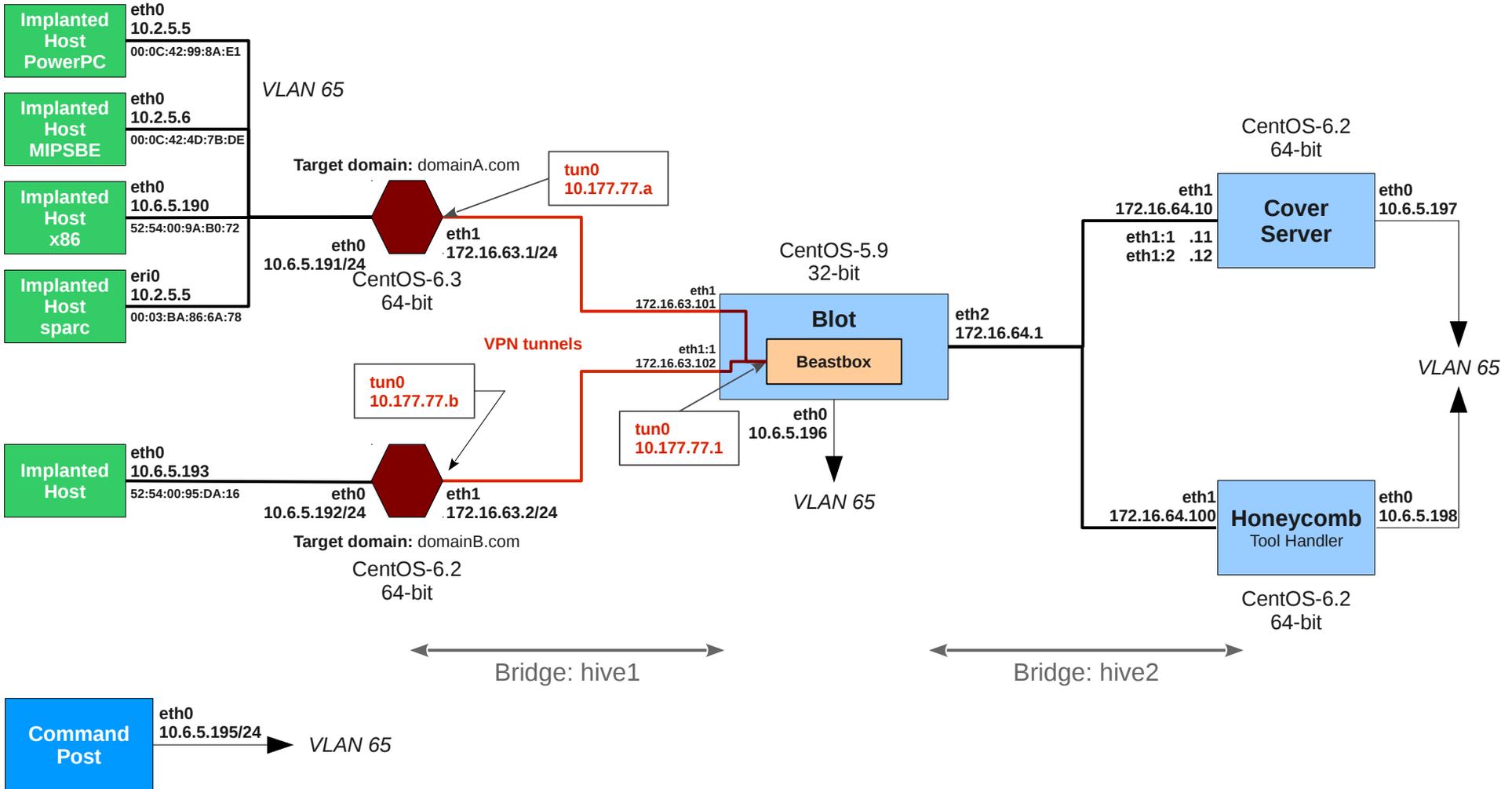
Hive Test Infrastructure

Implanted Hosts

VPS Servers

Proxy / Director

Response Servers



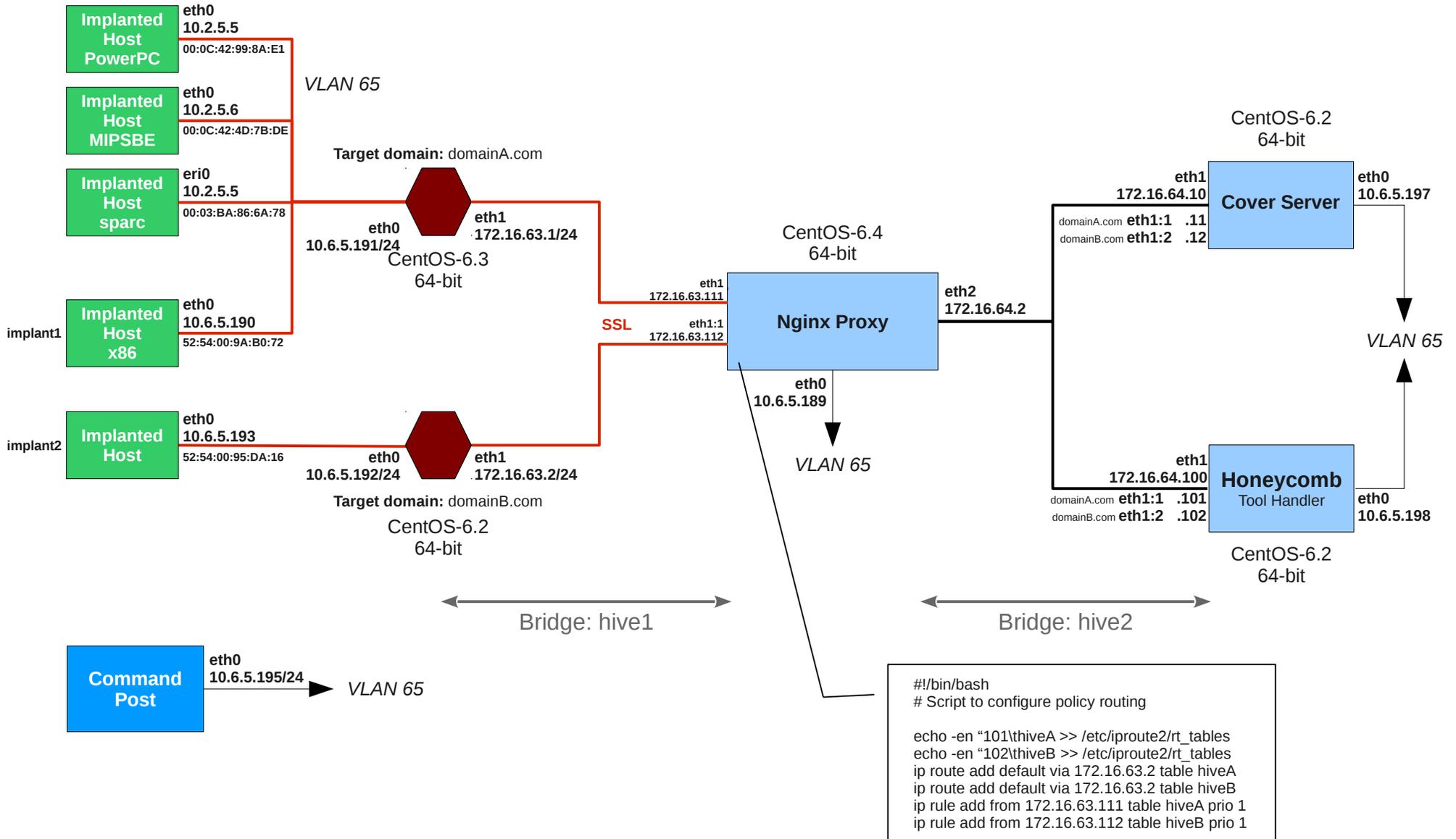
New Hive Test Infrastructure

Implanted Hosts

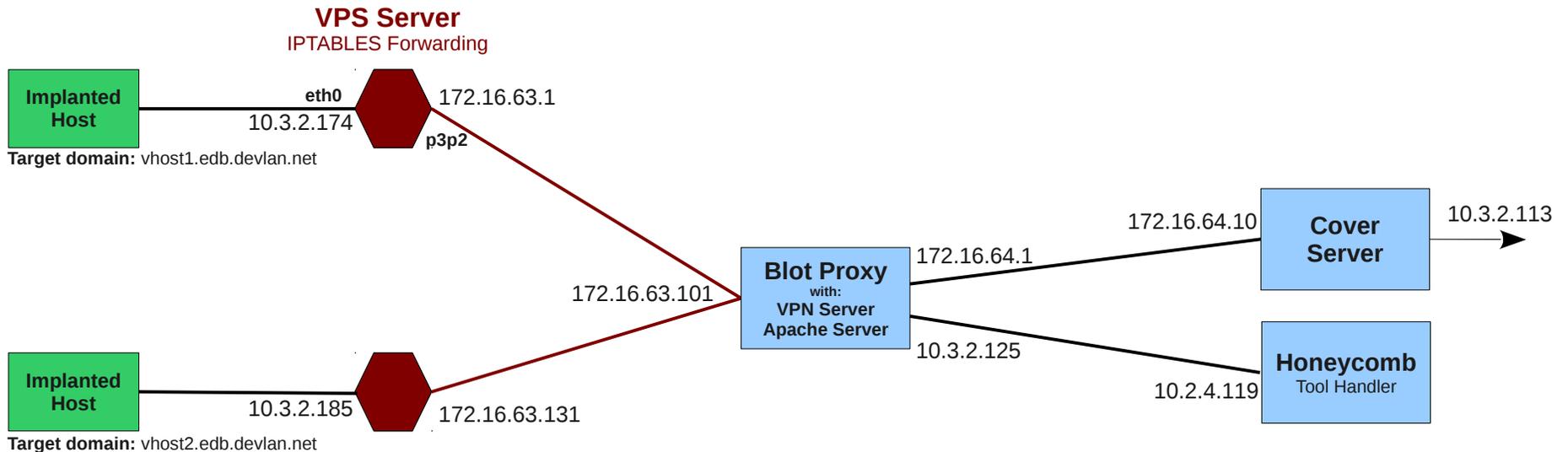
VPS Servers

Proxy / Director

Response Servers



Hive Beacon Test Infrastructure



VPS Server IPTABLES Configuration

```

iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT
DNAT
iptables -t nat -A PREROUTING -i eth0 -p tcp --sport 1024:65535 -d 10.3.2.174 --dport 53 -j DNAT --to-destination 172.16.63.101:443
iptables -t nat -A PREROUTING -i eth0 -p tcp --sport 1024:65535 -d 10.3.2.174 --dport 80 -j DNAT --to-destination 172.16.63.101:443
iptables -t nat -A PREROUTING -i eth0 -p tcp --sport 1024:65535 -d 10.3.2.174 --dport 443 -j DNAT --to-destination 172.16.63.101:443
FORWARDING
iptables -A FORWARD -i eth0 -o p3p2 -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i p3p2 -o eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i eth0 -o p3p2 -p tcp --sport 1024:65535 -d 172.16.63.101 --dport 53 -m state --state NEW -j ACCEPT
iptables -A FORWARD -i eth0 -o p3p2 -p tcp --sport 1024:65535 -d 172.16.63.101 --dport 80 -m state --state NEW -j ACCEPT
iptables -A FORWARD -i eth0 -o p3p2 -p tcp --sport 1024:65535 -d 172.16.63.101 --dport 443 -m state --state NEW -j ACCEPT
SNAT
iptables -t nat -A POSTROUTING -o p3p2 -j MASQUERADE

```


Hive Beacon Test Infrastructure

