infobip

Povezivanje distribuirane infrastrukture S2S VPN-ovima

Petar Pisnjak

20.04.2023.

Petar Pisnjak, Principal Engineer, Core Network - INFOBIP

- 7 years experience with Infobip
- Cisco, Mikrotik, Palo Alto, Lenovo network platforms
- Internal core routing
- Public peering with ISPs
- Network firewall security
- Cloud hybrid interconnectivity...

OUR GLOBAL PRESENCE

2020-2021

First investment

One Equity Partners

Strategic acquisitons

OpenMarket

INFOBIP Shift

anam

OUR GOAL IS TO INTERACT WITH EVERY MOBILE DEVICE ON EARTH

70+
Offices across the globe

€1.18bn+
Revenue FY2021E

190+
Countries

700+
Direct operator connections

64%
Global mobiles reached

3.5k+ Employees globally

60+ Nationalities

How we started

- Cisco ASA (Adaptive Security Appliance) – stateful firewall
  - Edge firewall (ACLs, core-dmz-outside, NATs)
  - Core router (between core subnets)
    - CPU limits due to traffic ammount
    - „hidden limits” due to connection count (new connections/s)
    - -> we soon moved to Nexus platform for CORE routing (/22 ?)
  - VPN gateway (terminating VPN to partners, between DCs)
    - Crypto based VPNs

Crypto based VPNs

- „industry standard”
- Access-lists -> crypto maps define local-remote hosts/subnets/sites (S2S)
  - Static and „hard to maintain”
  - NAT exempt (since ASA was also NAT device)
    - Problems with „object duplication”
  - NO proper REDUNDANCY
    - „there is 2 peer option...”
- ASDM configuration and management – simpler
  - CLI configuration and management – kinda complex
- Stable and reliable
- 100% compatibility with ASA HA failover – connection persistance

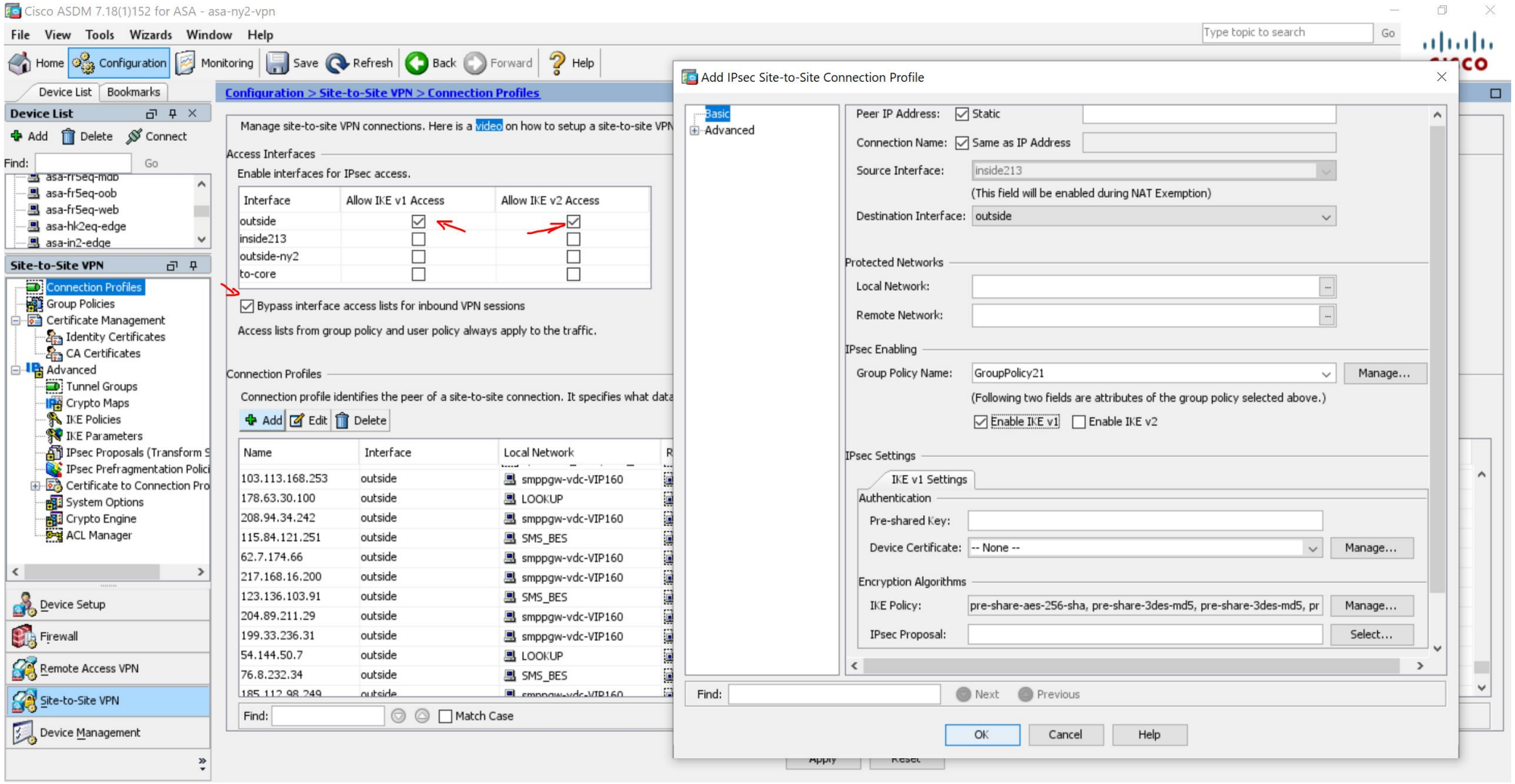
Crypto based VPN CLI

```
object-group network 12200_LOCAL_INFOBIP
    network-object host 62.140.31.156
    network-object host 62.140.31.58
object-group network 12200_REMOTE_PARTNER
    network-object host 194.197.246.102
access-list outside_cryptomap_12200 line 1 extended permit ip object-group 12200_LOCAL_INFOBIP object-group
12200_REMOTE_PARTNER
access-list outside_cryptomap_12200 line 1 remark PARTNER_NAME

group-policy GroupPolicy_194.197.246.124 internal
group-policy GroupPolicy_194.197.246.124 attributes
    vpn-tunnel-protocol ikev2
    exit
tunnel-group 194.197.246.124 type ipsec-l2l
tunnel-group 194.197.246.124 general-attributes
default-group-policy GroupPolicy_194.197.246.124
tunnel-group 194.197.246.124 ipsec-attributes
    ikev2 remote-authentication pre-shared-key PSK_placeholder
    ikev2 local-authentication pre-shared-key placeholder
    isakmp keepalive threshold 10 retry 2

crypto map outside_map 12200 match address outside_cryptomap_12200
crypto map outside_map 12200 set peer 194.197.246.124
crypto map outside_map 12200 set ikev2 ipsec-proposal AES256-SHA256
```

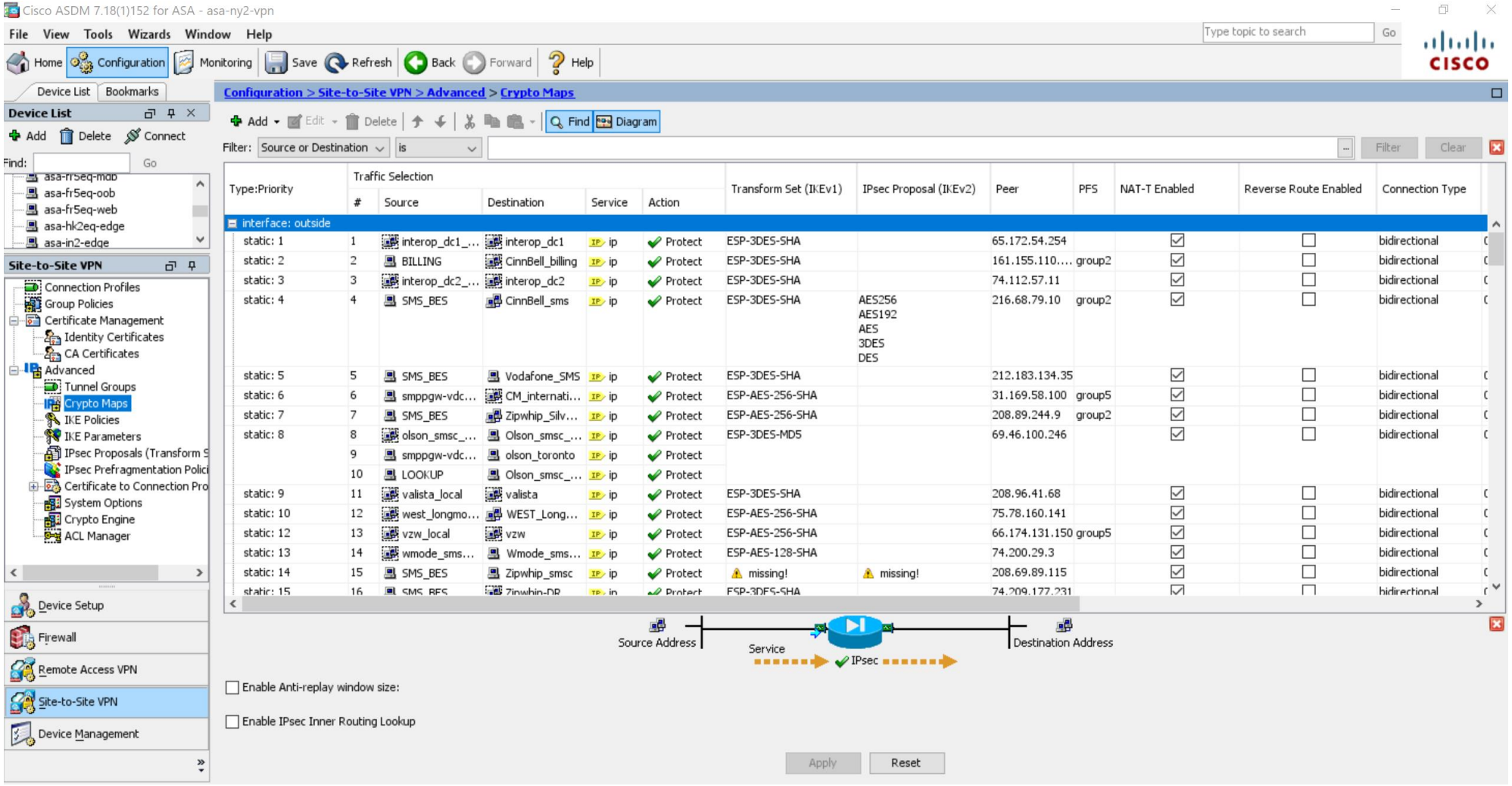
Phase 1 shared configuration:

```
crypto ikev1 policy 10
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
```

Crypto based VPN configuration via ASDM



Crypto based VPN management via ASDM



Cisco introduces VTI

- Virtual Tunnel Interface
- ~ 2017
- Some features unsupported or „semi-supported”
  - NAT – only as „any”
  - Cannot be bridged
  - Interface cannot be added to zone
  - Packet-tracer cannot set it as source interface
- IOS-XE supports only these types in newer versions...
- But it supports routing (we mostly tested with BGP)
  - Improved redundancy
  - Simplified routing
  - SD-WAN?

Configuration example – CLI only

```
crypto ipsec profile IPSECPROF
  set ikev1 transform-set ESP-AES-256-SHA
  set pfs group2
  set security-association lifetime kilobytes
 unlimited
  set security-association lifetime seconds 86400


tunnel-group 18.197.169.223 type ipsec-l2l
tunnel-group 18.197.169.223 general-attributes
 default-group-policy tunnelGP
tunnel-group 18.197.169.223 ipsec-attributes
 ikev1 pre-shared-key placeholder
 isakmp keepalive threshold 10 retry 2
```

```
int Tunnel1
    nameif vti1
    ip address 10.56.7.2 255.255.255.252
    tunnel source interface OUTSIDE
    tunnel destination 18.197.169.223
    tunnel mode ipsec ipv4
    tunnel protection ipsec profile IPSECPROF
```

Phase 1 same:

```
crypto ikev1 policy 10
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
```

Infobip introduces dynamic private routing - BGP

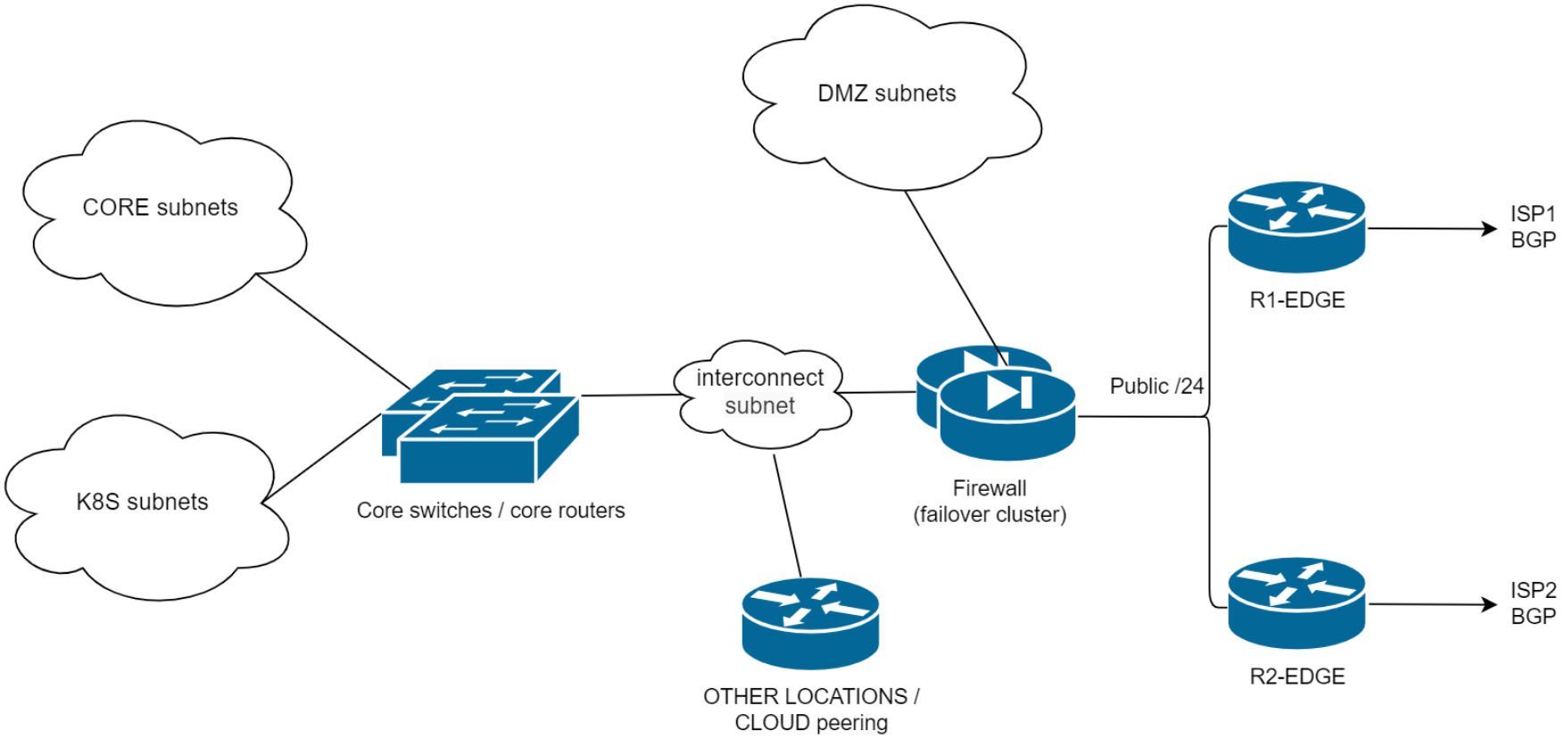
- We had extensive knowledge from public peerings
- OSPF
  - Easy to setup
  - Hard to troubleshoot?
- Using „private AS numbers”
  - Each „location” has its own AS number
  - Each „set of devices” has their own AS number
  - We can „track” path via AS path
  - ASAs in path – bad – we need to keep path symmetrical
    - Bogged down in local preferences
  - ASA HA failover bad with BGP... Connection reestablishing

Infobip introduces dynamic private routing - BGP

- Lessons were learned
  - Move from ASAs to „Route-based VPN routers” (license upgrade)
  - ECMP was possible in router-router paths
  - BFD for faster recovery
  - IP SLA – UDP probes for monitoring
  - Prefix-list filtering „le – ge”
    - We need to move away from „decadic” IP addressing
  - as-path filtering – bit tricky
  - Community strings – solution looking for problem?
    - Good for blackholing production traffic
  - MTU sizing ~ 1400 , MSS ~ 1360

Keep it as simple as possible

- Simple design is more robust and easier to maintain



Before we go

- IPv4 exhaustion... K8s main driver
- IPv6 in enterprise enviroment?
  - We just use cloud to do NAT IPv6 -> IPv4
  - Providers offer it per request
- Jumbo-frame adoption
  - MTU sizing is messy to upgrade
- ISP multihoming setup
  - Any advices on „standard BGP setup with ISPs”?
  - How to BETTER detect client side connection issues

WE ARE JUST STARTING

We are the **HUMBLE ENGINEERS** *led by our philosophy of* **LEARNING BY DOING** *and fuelled by our* **PASSION FOR TECHNOLOGY.** *We value* **CREATIVITY, PERSISTENCE** *and* **INNOVATION. INTEGRITY** *and living* **MEANINGFUL LIVES** *are the* **FOUNDATIONS** *of* **ALL OUR VALUES**

THANK YOU

infobip