



infobip



Povezivanje distribuirane infrastrukture S2S VPN-ovima

**Petar Pisnjak
20.04.2023.**



Petar Pisanjak, 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 acquisitions



OpenMarket



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 amount
 - „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 persistence



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

Cisco ASDM 7.18(1)152 for ASA - asa-ny2-vpn

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device List Bookmarks

Configuration > Site-to-Site VPN > Connection Profiles

Device List

Manage site-to-site VPN connections. Here is a [video](#) on how to setup a site-to-site VPN

Access Interfaces

Enable interfaces for IPsec access.

Interface	Allow IKE v1 Access	Allow IKE v2 Access
outside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
inside213	<input type="checkbox"/>	<input type="checkbox"/>
outside-ny2	<input type="checkbox"/>	<input type="checkbox"/>
to-core	<input type="checkbox"/>	<input type="checkbox"/>

Bypass interface access lists for inbound VPN sessions

Access lists from group policy and user policy always apply to the traffic.

Connection Profiles

Connection profile identifies the peer of a site-to-site connection. It specifies what data

Add Edit Delete

Name	Interface	Local Network
103.113.168.253	outside	smppgw-vdc-VIP160
178.63.30.100	outside	LOOKUP
208.94.34.242	outside	smppgw-vdc-VIP160
115.84.121.251	outside	SMS_BES
62.7.174.66	outside	smppgw-vdc-VIP160
217.168.16.200	outside	smppgw-vdc-VIP160
123.136.103.91	outside	SMS_BES
204.89.211.29	outside	smppgw-vdc-VIP160
199.33.236.31	outside	smppgw-vdc-VIP160
54.144.50.7	outside	LOOKUP
76.8.232.34	outside	SMS_BES
185.112.98.249	outside	smppgw-vdc-VIP160

Find: Match Case

Add IPsec Site-to-Site Connection Profile

Basic Advanced

Peer IP Address: Static

Connection Name: Same as IP Address

Source Interface: inside213

(This field will be enabled during NAT Exemption)

Destination Interface: outside

Protected Networks

Local Network:

Remote Network:

IPsec Enabling

Group Policy Name: GroupPolicy21

(Following two fields are attributes of the group policy selected above.)

Enable IKE v1 Enable IKE v2

IPsec Settings

IKE v1 Settings

Authentication

Pre-shared Key:

Device Certificate: -- None --

Encryption Algorithms

IKE Policy: pre-share-aes-256-sha, pre-share-3des-md5, pre-share-3des-md5, pr

IPsec Proposal:

Find:



Crypto based VPN management via ASDM

Cisco ASDM 7.18(1)152 for ASA - asa-ny2-vpn

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device List Bookmarks

Configuration > Site-to-Site VPN > Advanced > Crypto Maps

Device List: Add Delete Connect

Find: [] Go

Filter: Source or Destination is [] Filter Clear

Type:Priority	Traffic Selection	Transform Set (IKEv1)	IPsec Proposal (IKEv2)	Peer	PFS	NAT-T Enabled	Reverse Route Enabled	Connection Type					
#	Source	Destination	Service	Action									
interface: outside													
static: 1	1	interop_dc1_...	interop_dc1	IP ip	Protect	ESP-3DES-SHA		65.172.54.254			<input checked="" type="checkbox"/>		bidirectional
static: 2	2	BILLING	CinnBell_billing	IP ip	Protect	ESP-3DES-SHA		161.155.110....	group2		<input checked="" type="checkbox"/>		bidirectional
static: 3	3	interop_dc2_...	interop_dc2	IP ip	Protect	ESP-3DES-SHA		74.112.57.11			<input checked="" type="checkbox"/>		bidirectional
static: 4	4	SMS_BES	CinnBell_sms	IP ip	Protect	ESP-3DES-SHA	AES256 AES192 AES 3DES DES	216.68.79.10	group2		<input checked="" type="checkbox"/>		bidirectional
static: 5	5	SMS_BES	Vodafone_SMS	IP ip	Protect	ESP-3DES-SHA		212.183.134.35			<input checked="" type="checkbox"/>		bidirectional
static: 6	6	smppgw-vdc...	CM_internati...	IP ip	Protect	ESP-AES-256-SHA		31.169.58.100	group5		<input checked="" type="checkbox"/>		bidirectional
static: 7	7	SMS_BES	Zipwhip_Silv...	IP ip	Protect	ESP-AES-256-SHA		208.89.244.9	group2		<input checked="" type="checkbox"/>		bidirectional
static: 8	8	olson_smsc_...	Olson_smsc_...	IP ip	Protect	ESP-3DES-MD5		69.46.100.246			<input checked="" type="checkbox"/>		bidirectional
static: 9	11	LOOKUP	Olson_smsc_...	IP ip	Protect								
static: 9	11	valista_local	valista	IP ip	Protect	ESP-3DES-SHA		208.96.41.68			<input checked="" type="checkbox"/>		bidirectional
static: 10	12	west_longmo...	WEST_Long...	IP ip	Protect	ESP-AES-256-SHA		75.78.160.141			<input checked="" type="checkbox"/>		bidirectional
static: 12	13	vzw_local	vzw	IP ip	Protect	ESP-AES-256-SHA		66.174.131.150	group5		<input checked="" type="checkbox"/>		bidirectional
static: 13	14	wmode_sms...	Wmode_sms...	IP ip	Protect	ESP-AES-128-SHA		74.200.29.3			<input checked="" type="checkbox"/>		bidirectional
static: 14	15	SMS_BES	Zipwhip_smsc	IP ip	Protect		missing!	208.69.89.115			<input checked="" type="checkbox"/>		bidirectional
static: 15	16	SMS_BES	Zipwhip-DR	IP ip	Protect	ESP-3DES-SHA		74.209.177.231			<input checked="" type="checkbox"/>		bidirectional

Source Address | Service | Destination Address

Enable Anti-replay window size:

Enable IPsec Inner Routing Lookup:

Apply Reset



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



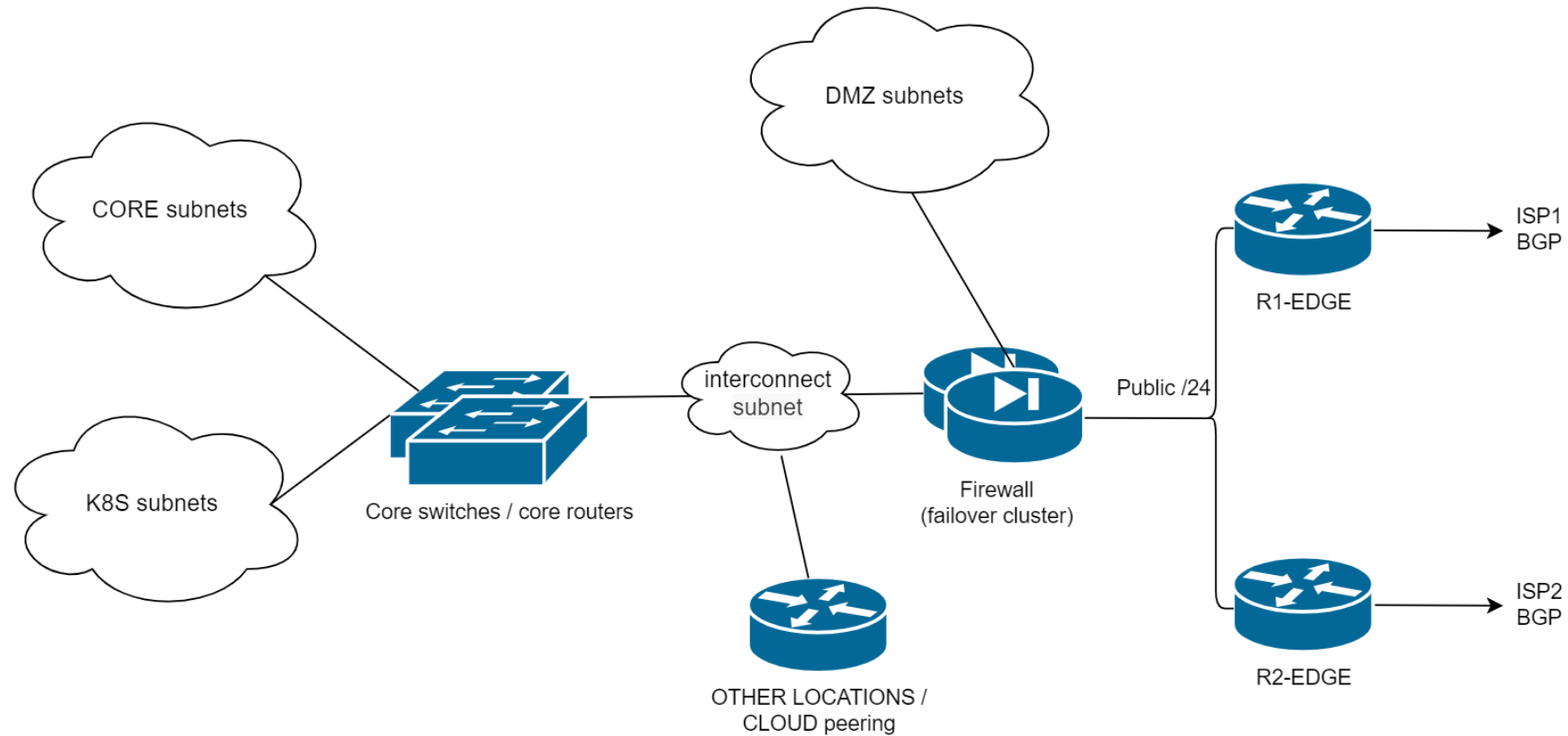
Infobip introduces dynamic private routing - BGP

- 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 environment?
 - ▶ 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