Secure your cloud with the IPsec BOSH release

Dr. Stefan Lay, Development Expert, SAP SE
Agenda

Eve and Mallory at SAP Cloud Platform

IPsec and TLS

The IPsec BOSH release

Demo: IPsec on BOSH-lite
Eve and Mallory at SAP Cloud Platform

Multi Customer Cloud

Diego Cell

Container

Customer App Process

http

Backing Service (Connectivity Agent)

Agent Process

Secure Tunnel

On Premise

Customer Backend
Eve and Mallory at SAP Cloud Platform

Multi Customer Cloud

Diego cell

Container

Customer App Process

Eve

Backing Service (Connectivity Agent)

Agent Process
IPsec and TLS

DNSSEC, EAP, RADIUS, SSH, Kerberos

TLS

IPsec

802.1X(EAPoL), 802.11/WPA2
## IPsec and TLS

<table>
<thead>
<tr>
<th></th>
<th>IPSec</th>
<th>TLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption between</td>
<td>Hosts</td>
<td>Processes</td>
</tr>
<tr>
<td>Widely used for</td>
<td>VPNs</td>
<td>Web Apps</td>
</tr>
<tr>
<td>Configured in</td>
<td>OS kernel</td>
<td>Buildpack/App</td>
</tr>
<tr>
<td>Configure Certs in Buildpack</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Application Protocols</td>
<td>Protocols based on IP</td>
<td>Protocols based on TLS</td>
</tr>
</tbody>
</table>
IPsec and TLS

- Built into Linux Kernel (since 2.6)
- Tools available at ipsec-tools (http://ipsec-tools.sourceforge.net/)
- Policies are set in a SPD (Security Policy Database):

```bash
$ setkey -P -D
10.244.0.34[any] 10.244.0.35[any] 255
out prio def ipsec
esp/transport//require
...
```

- Opt-In: Ipsec is only used for hosts configured in SPD
IPsec: Two phases

• Establishment phase: a security association is built
• Data exchange phase:
  different types of encapsulation schemes:
  • Authentication Header (AH)
  • Encapsulating Security Payload (ESP)
IPsec: Establishment phase

- Establishment phase: Entry in Security Association Database (SAD)
- Internet Key Exchange (IKE) protocol (UDP port 500)
- Trust via Shared Secret, Plain RSA or Certificates
- SAD-entry:

```
$ setkey -D
10.244.0.34 10.244.0.35
est esp mode=transport spi=82530899(0x04eb5253) reqid=0(0x00000000)
E: aes-cbc 4cd1fc34 69f816f0 b39e85f1 a9a265f9
A: hmac-sha256 ea6b3b5c bcb4eb97 b0068afd f4d45cd 75070d6a
   1a18efcb ed980f21 169b1d1a
...```
IPsec: Data exchange phase

Regular IP

<table>
<thead>
<tr>
<th>IPv4 Header</th>
<th>TCP Header</th>
<th>Data</th>
</tr>
</thead>
</table>

ESP Transfer mode

<table>
<thead>
<tr>
<th>IPv4 Header</th>
<th>ESP Header</th>
<th>TCP Header</th>
<th>Data</th>
<th>ESP Trailer</th>
<th>ESP ICV</th>
</tr>
</thead>
</table>

Protocol: 50
SPI: 82530899
The IPsec BOSH release

- Enable IPsec communication between hosts setup with BOSH
- Open Source under Apache License 2.0
- [https://github.com/SAP/ipsec-release](https://github.com/SAP/ipsec-release)
- Forked from [https://github.com/CloudCredo/bosh-ipsec](https://github.com/CloudCredo/bosh-ipsec)
- Uses setkey from ipsec-tools for Security Police Database
- Uses racoon with certificates from ipsec-tools for IKE
The IPsec BOSH-Release

• IPsec is co-deployed on VMs:

```yaml
jobs:
- name: racoon
  release: ipsec
```
The IPsec BOSH-Release

• Configuration:

```yaml
properties:
raccoon:
  disabled: false
  level: require
ports:
  - name: default
    targets:
      - 10.244.0.35
certificate_authority_cert: ...
certificate_authority_private_key: ...
```
DEMO
Lessons Learned

- Easy to setup
- Very stable, no issues observed
- No officially signed certificate needed
- No TLS configuration overhead for App developers
- Configuration of ports (IP addresses) can get complicated
- More complex for HA-Setup with Load Balancer
Q & A
Appendix: Dumping tcp traffic

iptables -t mangle -I PREROUTING -m policy --pol ipsec --dir in -j NFLOG --nflog-group 5
iptables -t mangle -I POSTROUTING -m policy --pol ipsec --dir out -j NFLOG --nflog-group 5
tcpdump -n -i nflog:5 -w test.log