Deep Dive: Virtual Private Cloud

Julien Simon

Principal Technical Evangelist

julsimon@amazon.fr

@julsimon

amazon web services | Pop-up Loft TEL AVIV

aws vpc --expert-mode

Agenda

172.16.0.0
172.16.1.0
172.16.2.0

Routing
& Private links

VPC Peering

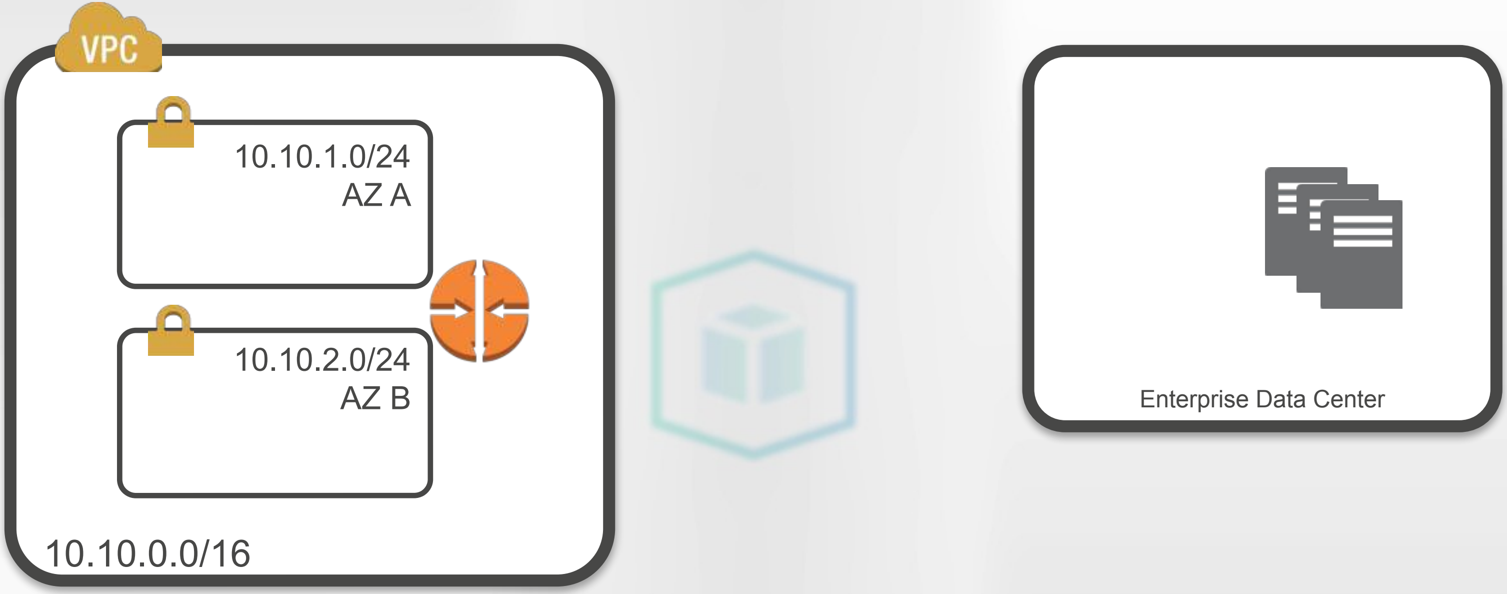
Enhanced
Networking

Routing & Private Links

Building an Hybrid Architecture

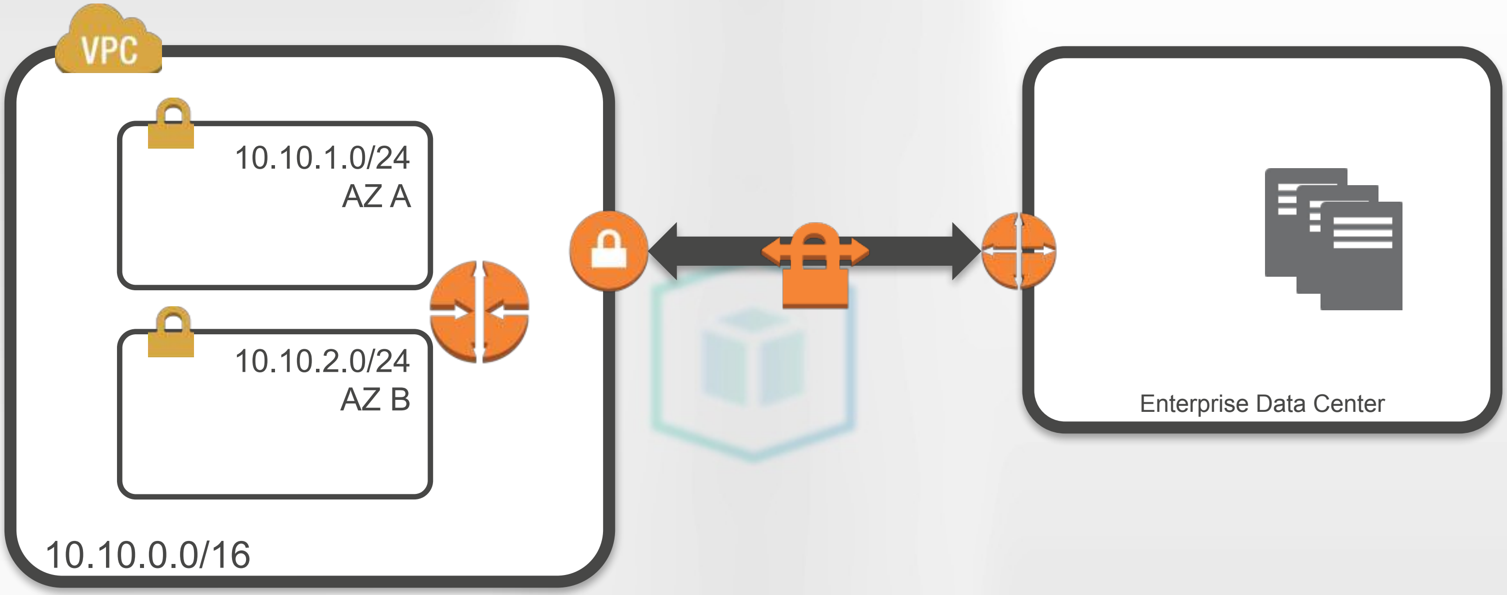
Enterprise Data Center

Create a VPC



```
aws ec2 create-vpc --cidr 10.10.0.0/16
aws ec2 create-subnet --vpc vpc-c15180a4 --cidr 10.10.1.0/24 --a us-west-2a
aws ec2 create-subnet --vpc vpc-c15180a4 --cidr 10.10.2.0/24 --a us-west-2b
```

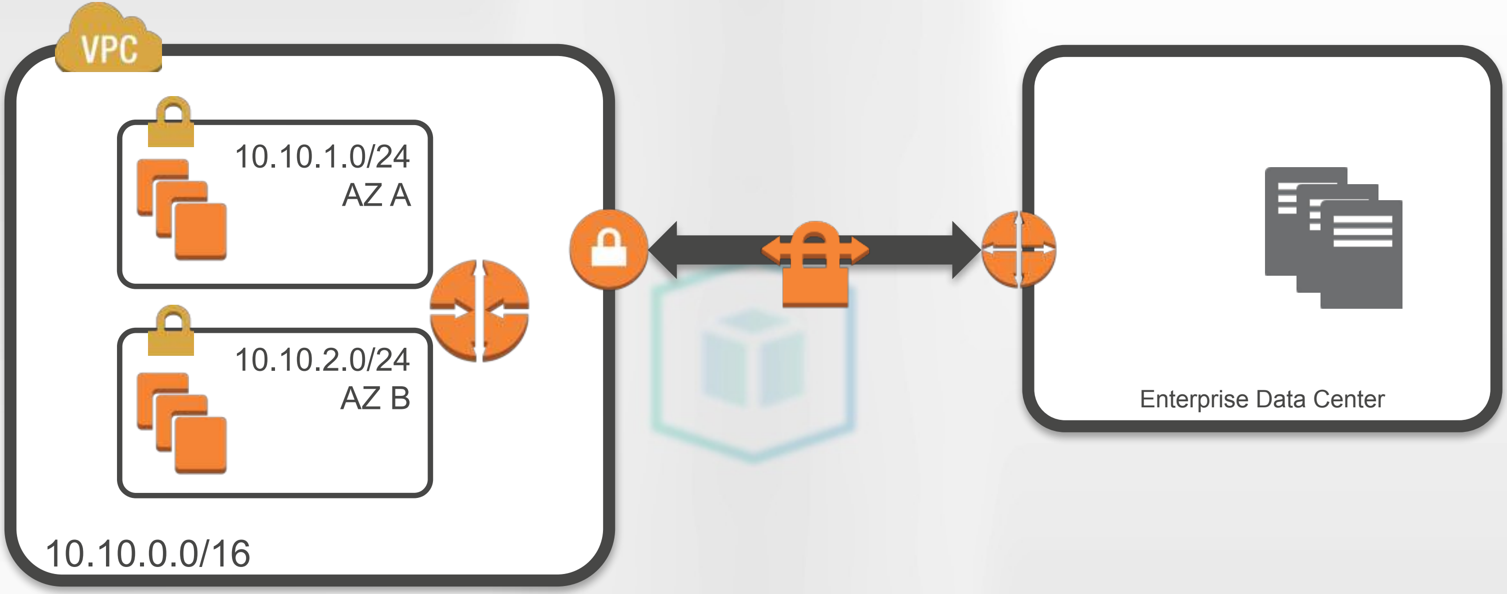
Create a VPN connection



```
aws ec2 create-vpn-gateway --type ipsec.1
aws ec2 attach-vpn-gateway --vpn vgw-f9da06e7 --vpc vpc-c15180a4
aws ec2 create-customer-gateway --type ipsec.1 --public 54.64.1.2 --bgp 6500
aws ec2 create-vpn-connection --vpn vgw-f9da06e7 --cust cgw-f4d905ea --t ipsec.1
```

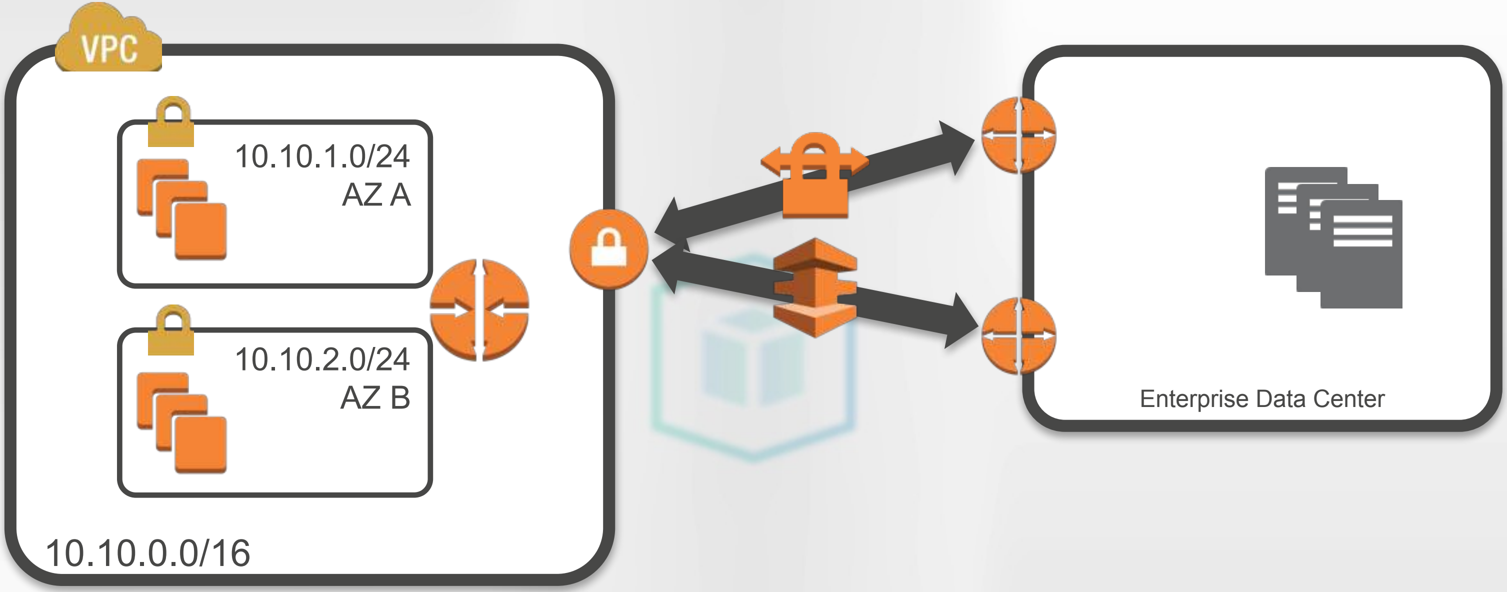
http://docs.aws.amazon.com/fr_fr/AmazonVPC/latest/UserGuide/VPC_VPN.html
http://docs.aws.amazon.com/fr_fr/AmazonVPC/latest/NetworkAdminGuide/Introduction.html

Launch instances



```
aws ec2 run-instances --image ami-d636bde6 --sub subnet-d83d91bd --count 3
aws ec2 run-instances --image ami-d636bde6 --sub subnet-b734f6c0 --count 3
```

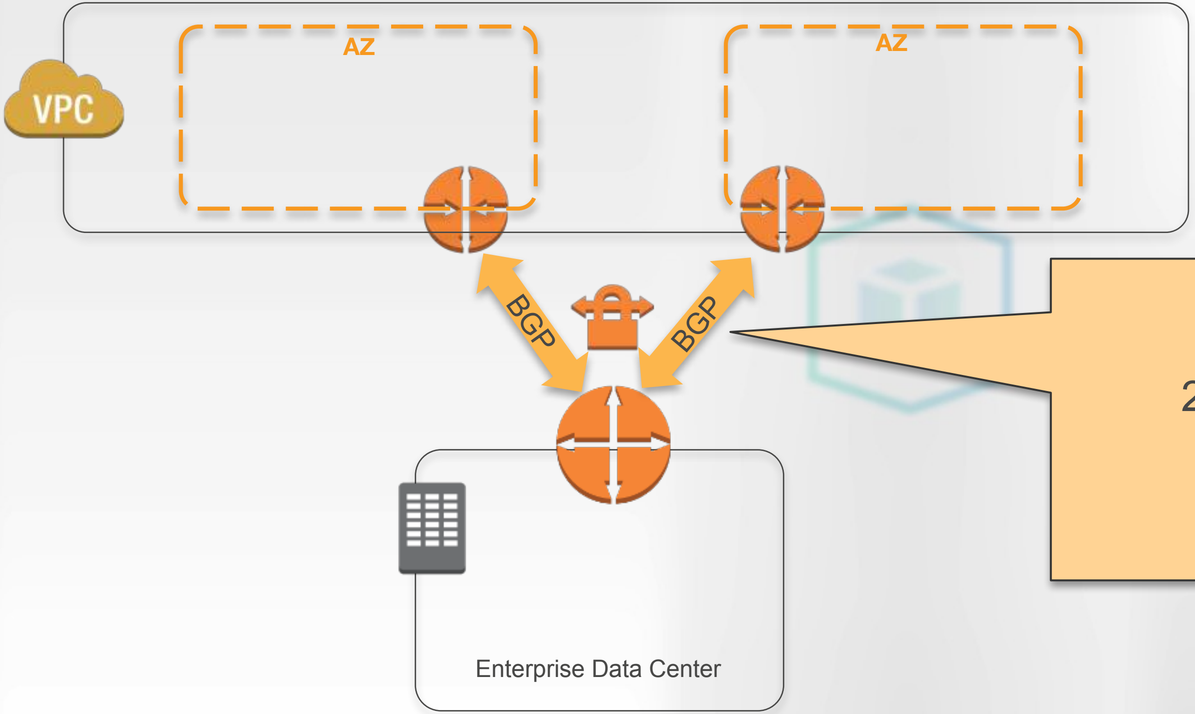
Using AWS Direct Connect



```
aws directconnect create-connection --loc EqSE2 --b 1Gbps --conn My_First
aws directconnect create-private-virtual-interface --conn dxcon-fgp13h2s --new
virtualInterfaceName=Foo, vlan=10, asn=60, authKey=testing,
amazonAddress=192.168.0.1/24, customerAddress=192.168.0.2/24,
virtualGatewayId=vgw-f9da06e7
```

http://www.slideshare.net/JulienSIMON5/an-introduction-to-aws-direct-connect

Best pratices for remote connections



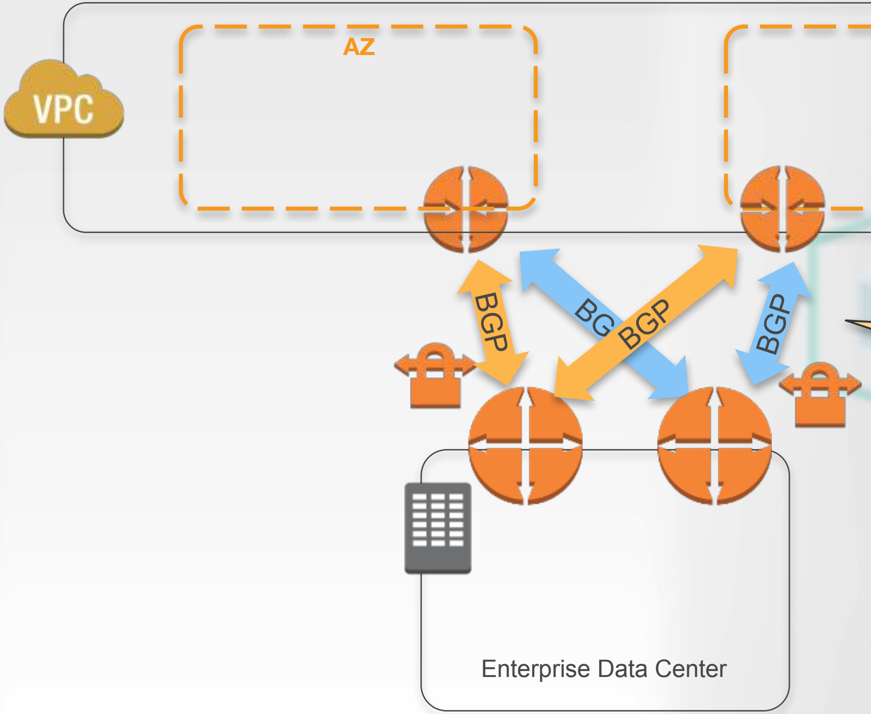
Each VPN link uses
2 redundant IPSec tunnels.

Use BGP for routing.

Availability : Good

🟧🟧🟧⬜⬜

Best pratices for remote connections

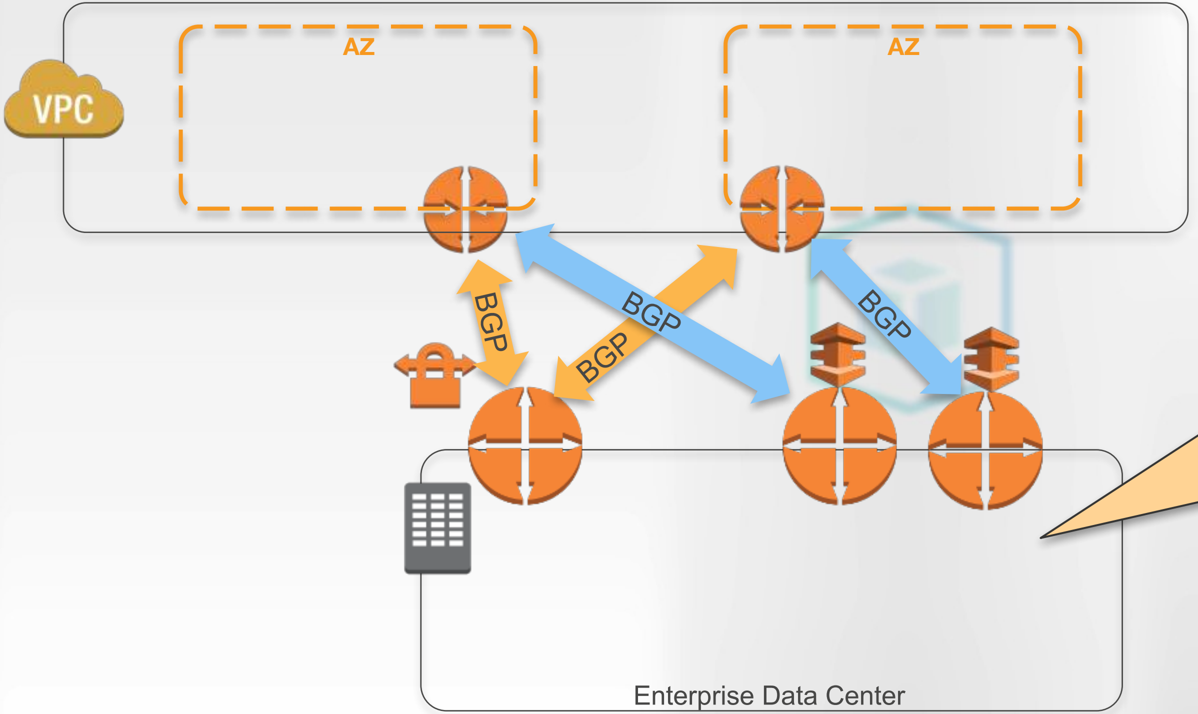


2 VPN connections
(4 IPSec tunnels total)
on different devices
→ no SPOF

Availability : Better

🟩🟩🟩🟩⬜

Best pratices for remote connections



Redudant Direct Connect connections + backup VPN

BGP selects best route

Availability: Best

🟩🟩🟩🟩🟩

https://aws.amazon.com/fr/directconnect/partners/

Route selection (customer site → VGW)

When multiple connections are available, multiple routes to the VPN Gateway will exist on your router.

- You have to manage this yourself ☺
- Static routes: what about failover?
- BGP is the best option
  - Active / passive: you can favor one path, e.g. DX > VPN (Cisco: *WEIGHT* and *LOCAL_PREFERENCE* attributes)
  - Active / Active : you can set up BGP Multipath (Cisco : *BGP Link Bandwidth*)

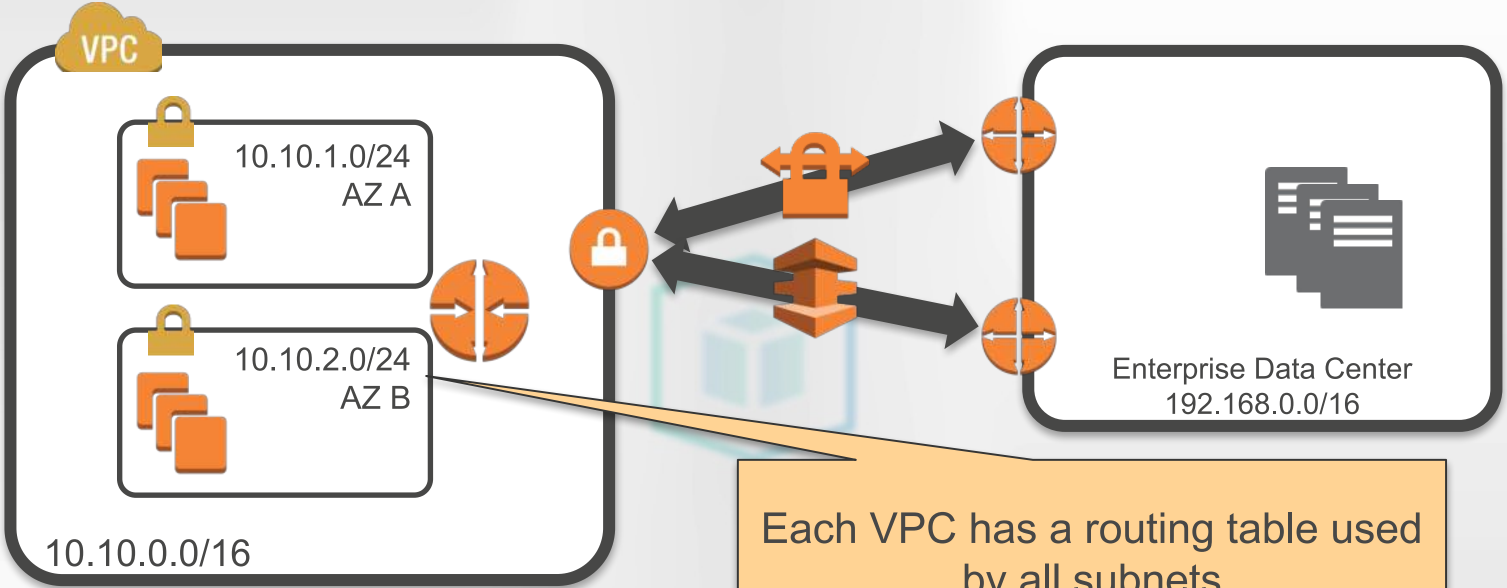
Route selection (VGW → customer site)

When multiple connections are available, multiple routes to the same customer destination may exist on the VGW.

1. The most specific IP Prefix is favored (10.0.0.0/24 > 10.0.0.0/16)
2. Identical prefix? Static routes are favored over BGP routes
3. Multiple BGP routes? The shortest AS path is favored
   - You can use the AS_PATH prefix to penalize a route
   - If AS paths have the same length, their origin will be taken into account (IGP > EGP > unknown)

http://docs.aws.amazon.com/fr_fr/AmazonVPC/latest/NetworkAdminGuide/Introduction.html#MultipleVPNConnections

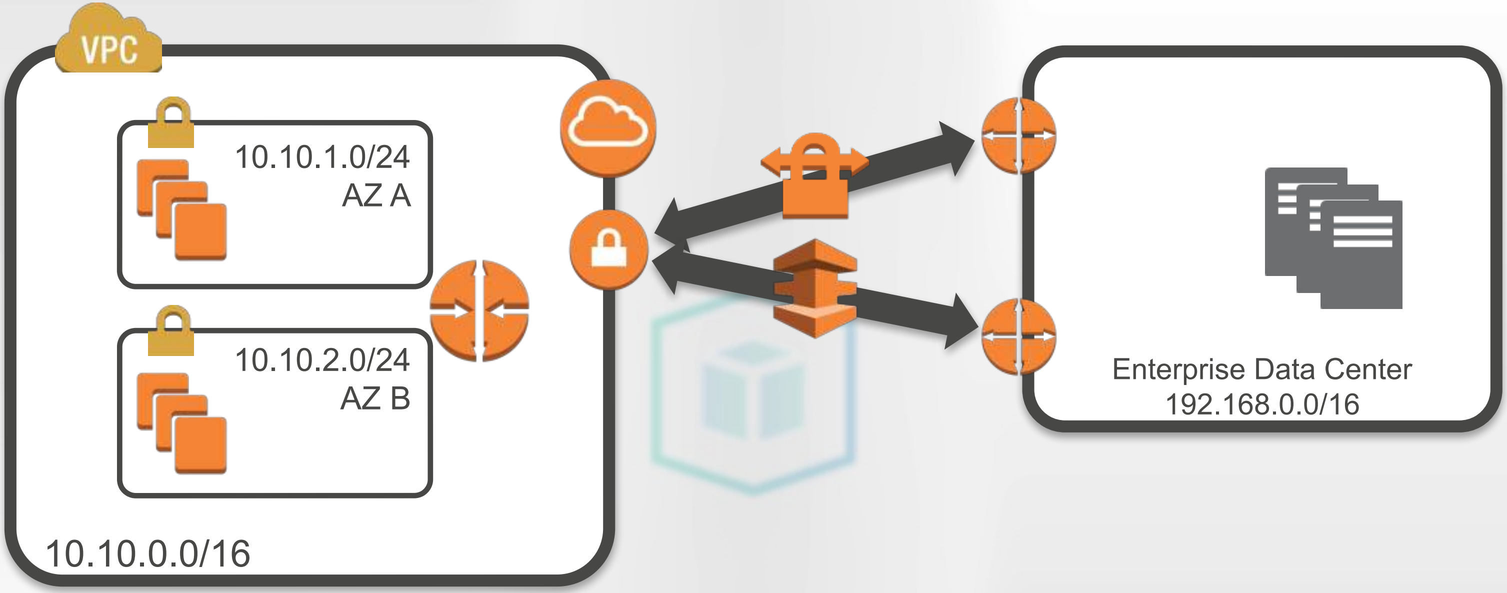
Routing: default route



Each VPC has a routing table used by all subnets

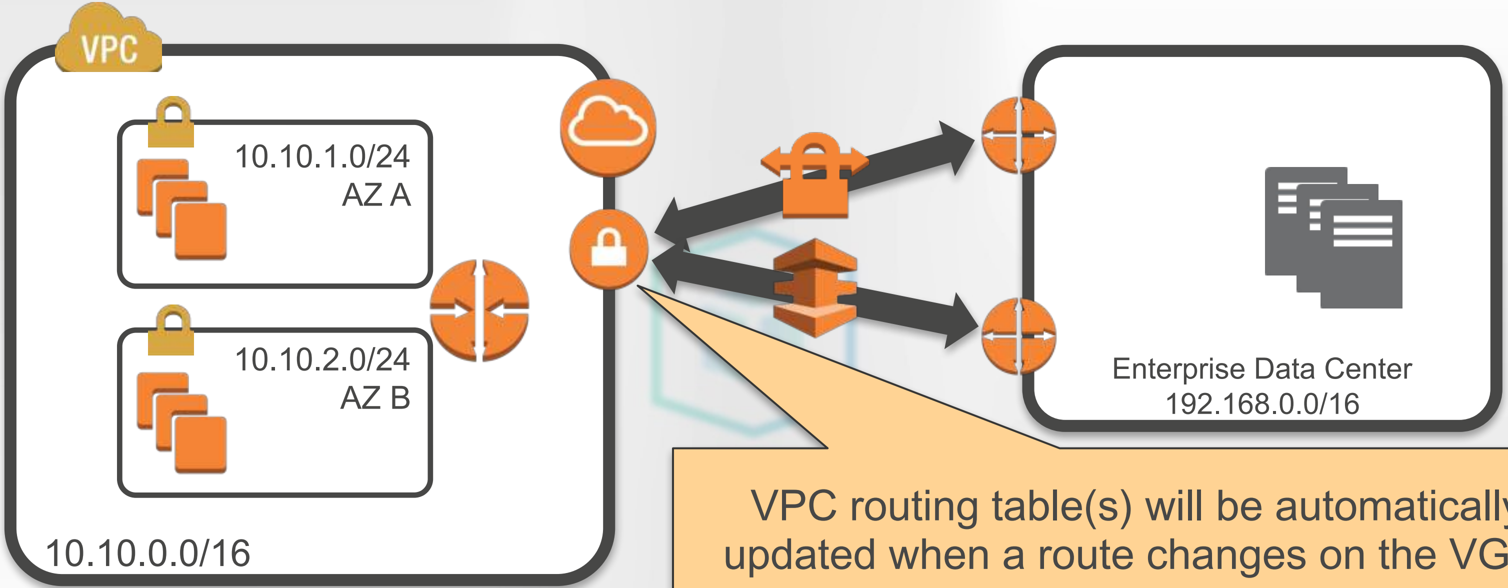
```
aws ec2 create-route --ro rtb-ef36e58a --dest 0.0.0.0/0 --gateway-id vgw-f9da06e7
```

Routing: private and public connectivity



```
aws ec2 create-internet-gateway
aws ec2 attach-internet-gateway --internet igw-5a1ae13f --vpc vpc-c15180a4
aws ec2 delete-route --ro rtb-ef36e58a --dest 0.0.0.0/0
aws ec2 create-route --ro rtb-ef36e58a --dest 0.0.0.0/0 --gateway-id igw-5a1ae13f
aws ec2 create-route --ro rtb-ef36e58a --dest 192.168.0.0/16 --gateway-id vgw-f9da06e7
```

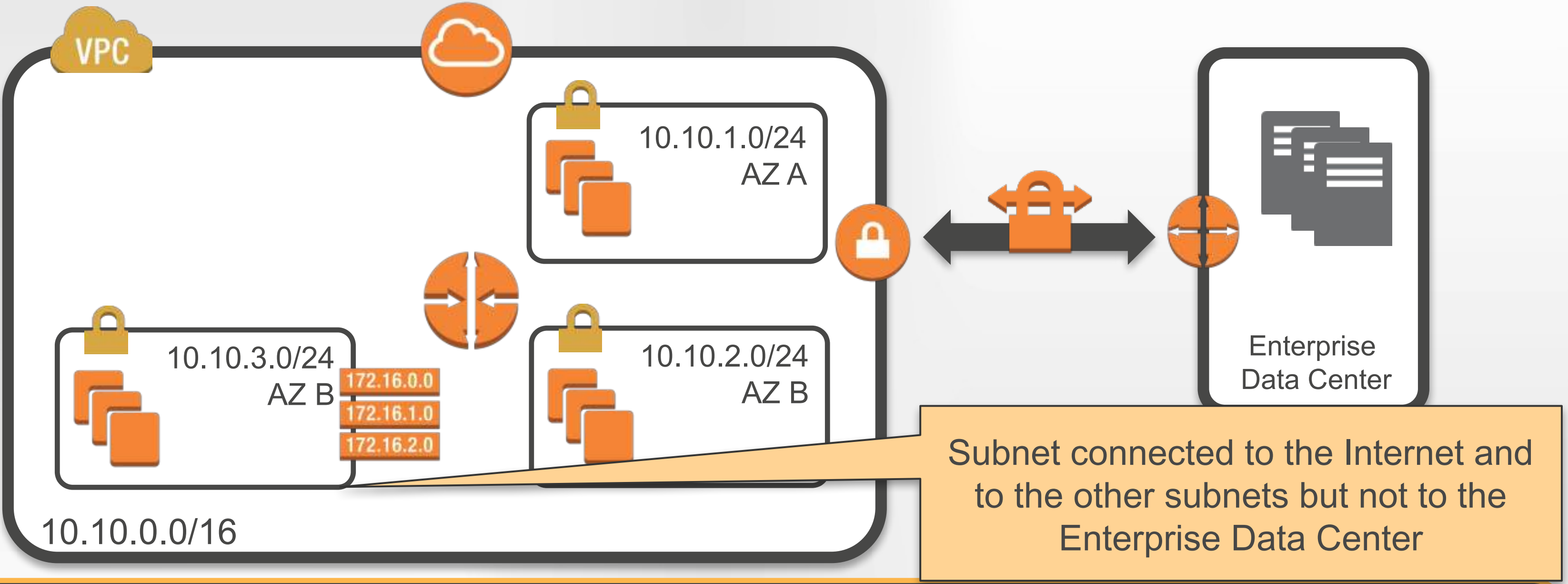
Routing: propagating routes from the VGW to the VPC



VPC routing table(s) will be automatically updated when a route changes on the VGW

```
aws ec2 delete-route --ro rtb-ef36e58a --dest 192.168.0.0/16
aws ec2 enable-vgw-route-propagation --ro rtb-ef36e58a --gateway-id vgw-f9da06e7
```

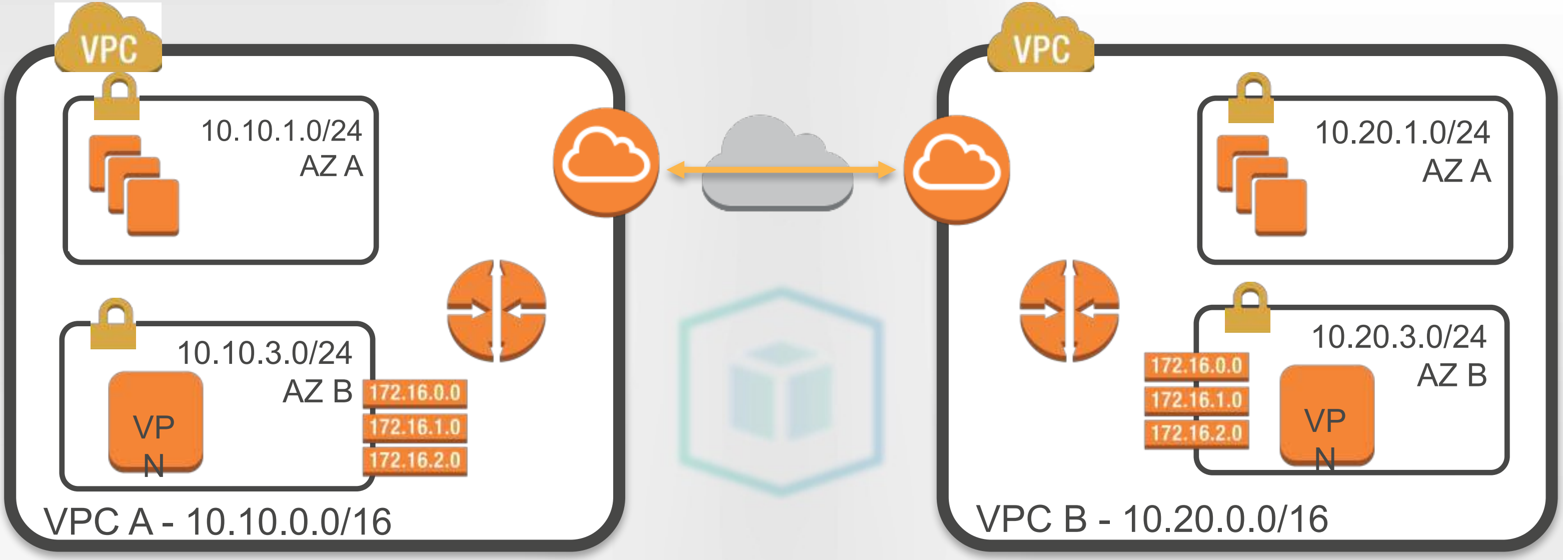
Routing: subnet-specific routing table



Subnet connected to the Internet and to the other subnets but not to the Enterprise Data Center

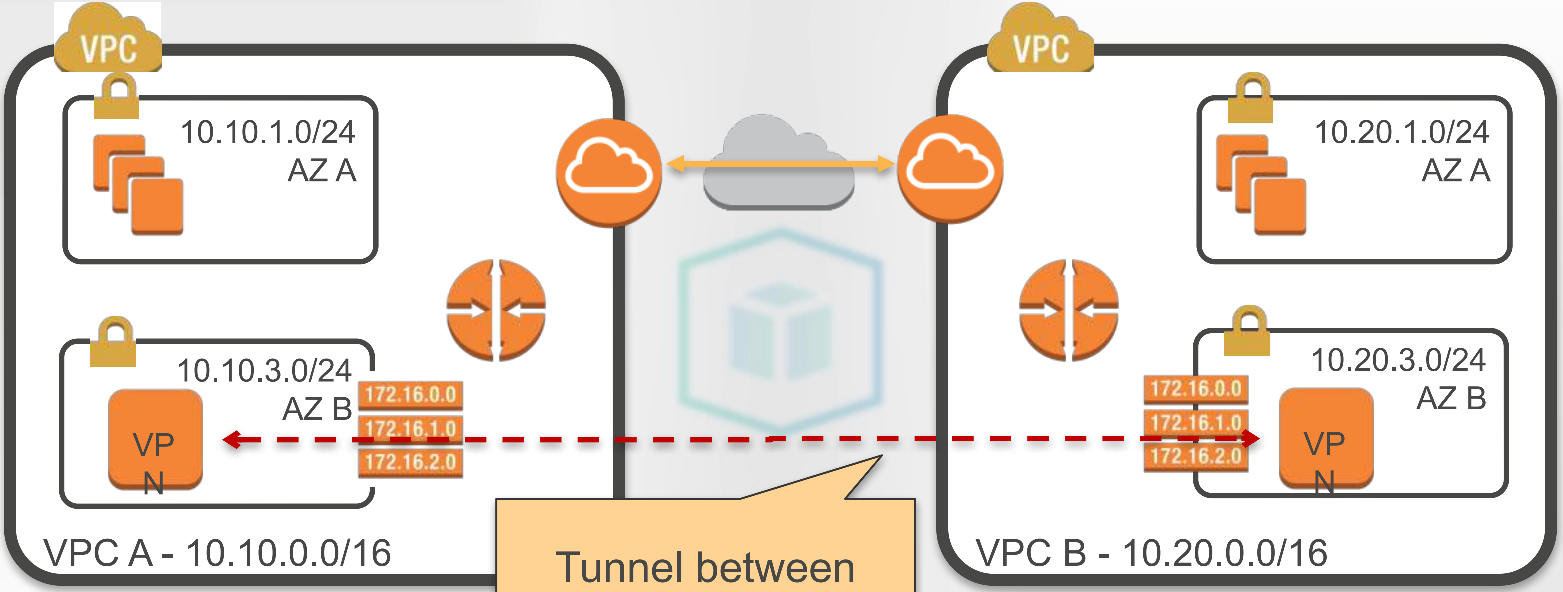
```
aws ec2 create-subnet --vpc vpc-c15180a4 --cidr 10.10.3.0/24 --a us-west-2b
aws ec2 create-route-table --vpc vpc-c15180a4
aws ec2 associate-route-table --ro rtb-fc61b299 --subnet subnet-60975a17
aws ec2 create-route --ro rtb-ef36e58a --dest 0.0.0.0/0 --gateway-id igw-5a1ae13f
```

Setting up a software VPN in EC2 across VPCs



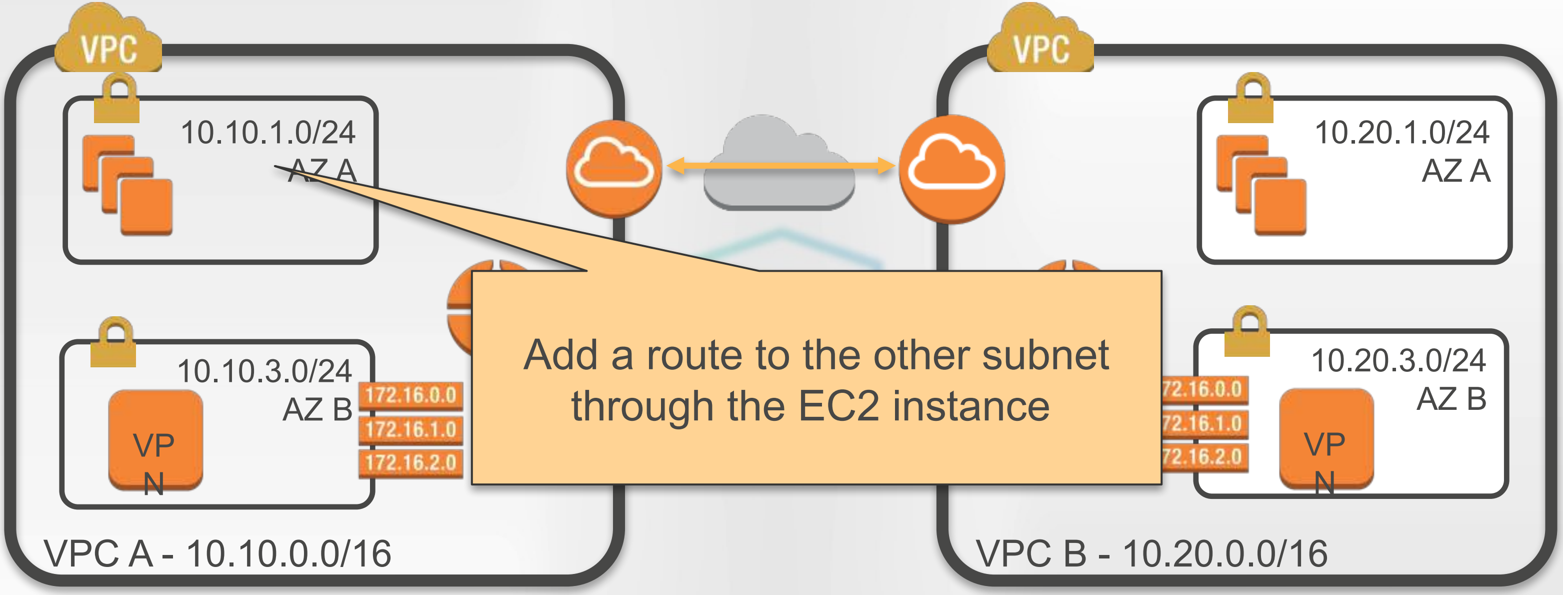
```
# VPC A
aws ec2 modify-network-interface-attribute --net eni-f832afcc --no-source-dest-check

# VPC B
aws ec2 modify-network-interface-attribute --net eni-9c1b693a --no-source-dest-check
```

Setting up a software VPN in EC2 across VPCs



Tunnel between these instances

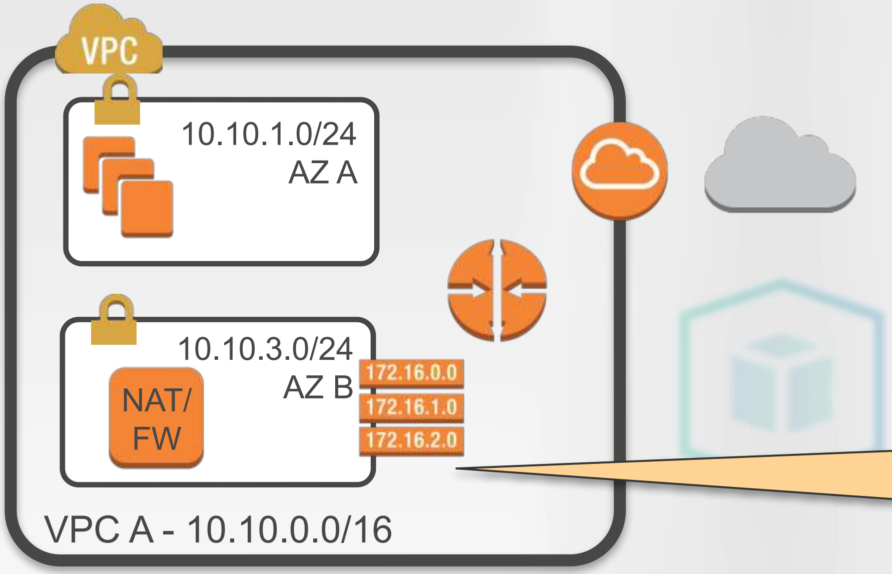
Setting up a software VPN in EC2 across VPCs



Add a route to the other subnet through the EC2 instance

```
# VPC A
aws ec2 create-route --ro rtb-ef36e58a --dest 10.20.0.0/16 --instance-id i-f832afcc

# VPC B
aws ec2 create-route --ro rtb-67a2b31c --dest 10.10.0.0/16 --instance-id i-9c1b693a
```

Setting up a software firewall on EC2



All subnet traffic goes through the NAT/FW before going to the Internet

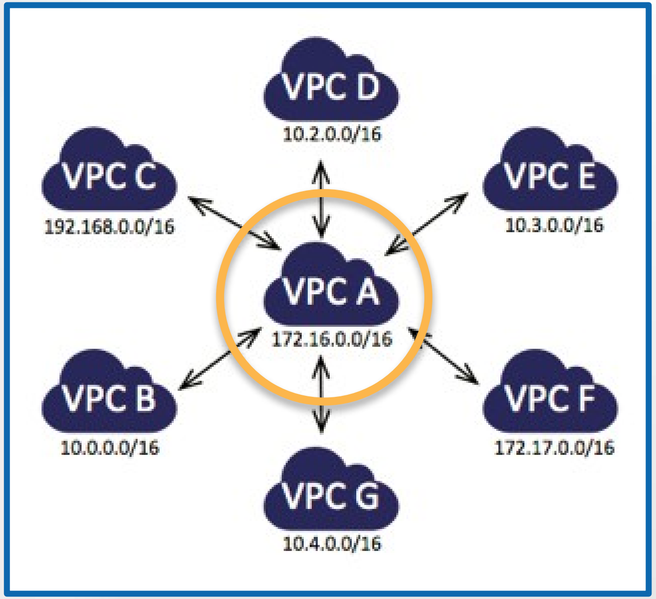
```
aws ec2 modify-network-interface-attribute --net eni-f832afcc --no-source-dest-check

# The default routing table sends traffic to the NAT/FW instance
aws ec2 create-route --ro rtb-ef36e58a --dest 0.0.0.0/0 --instance-id i-f832afcc

# Route from 10.10.3.0/24 to the Internet
aws ec2 create-route --ro rtb-67a2b31c --dest 0.0.0.0/0 --gateway-id igw-5a1ae13f
```

VPC Peering

Sharing a service VPC through peering

Core services

- Authentication / Directory
- Monitoring
- Logging
- Remote management
- Security audits

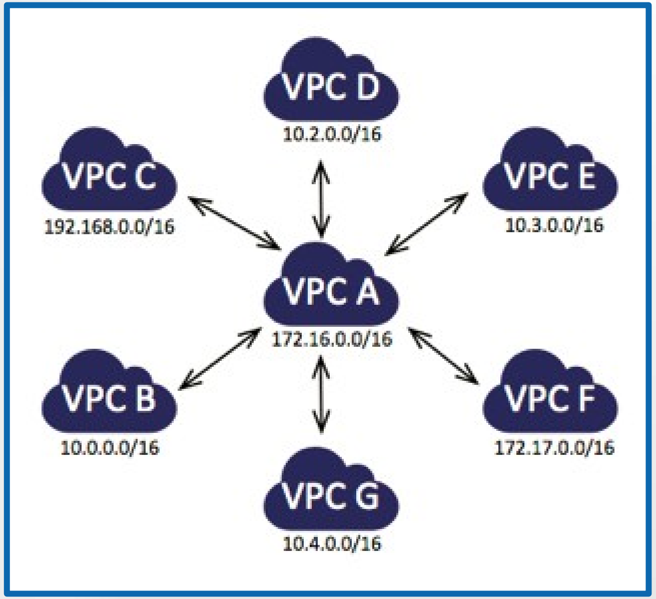


Partitioning your infrastructure with peering

Development : VPC B

Test : VPC C

Production : VPC D



VPC peering – things you should know

VPCs should be in the same region.

VPC address ranges must not overlap.

Routing: use private IP addresses - IPv4 or IPv6 (since December 2016).

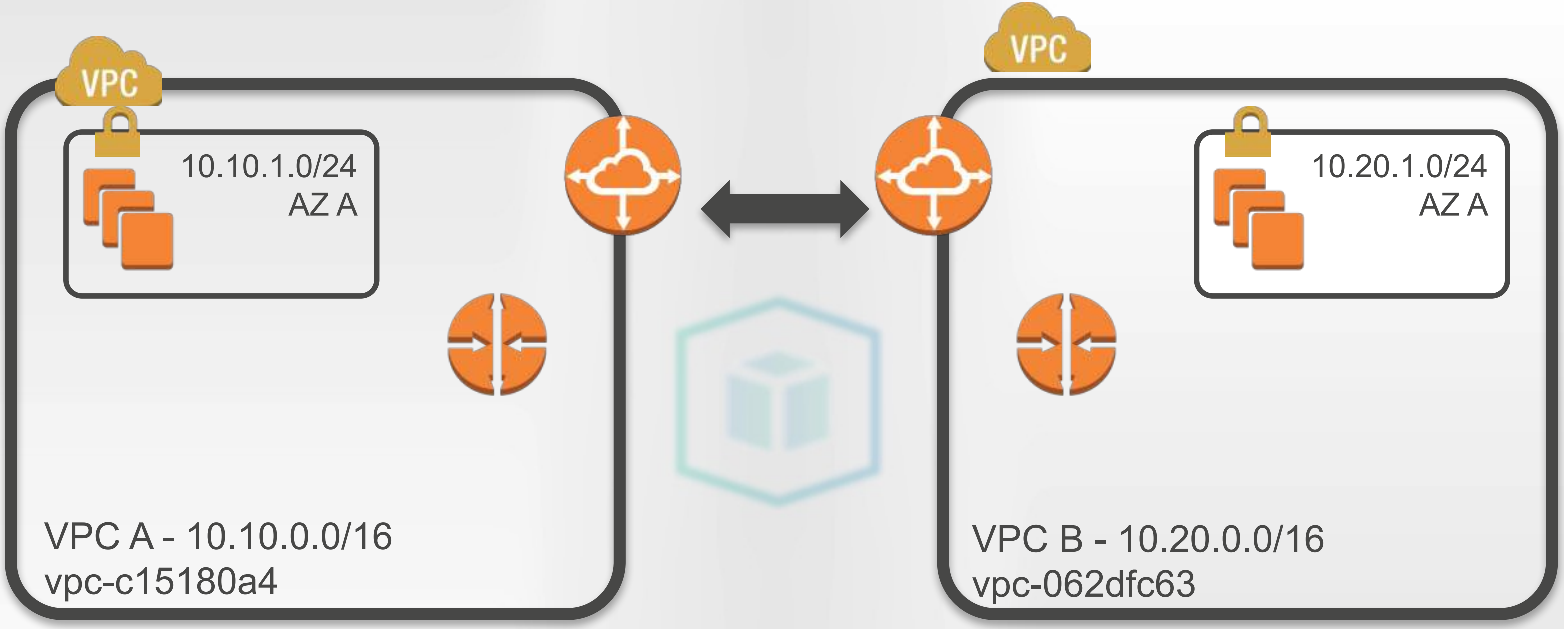
Security groups: since March 2016, you can reference them across VPCs.

DNS: since July 2016, you can resolve private addresses across VPCs.

No transitivity for VPN peering or Direct Connect

- Example : A peers with B, B peers with C → A doesn't peer with C
- Solution : set up peering explicitely between A and C

VPC peering in the same account



10.10.1.0/24
AZ A

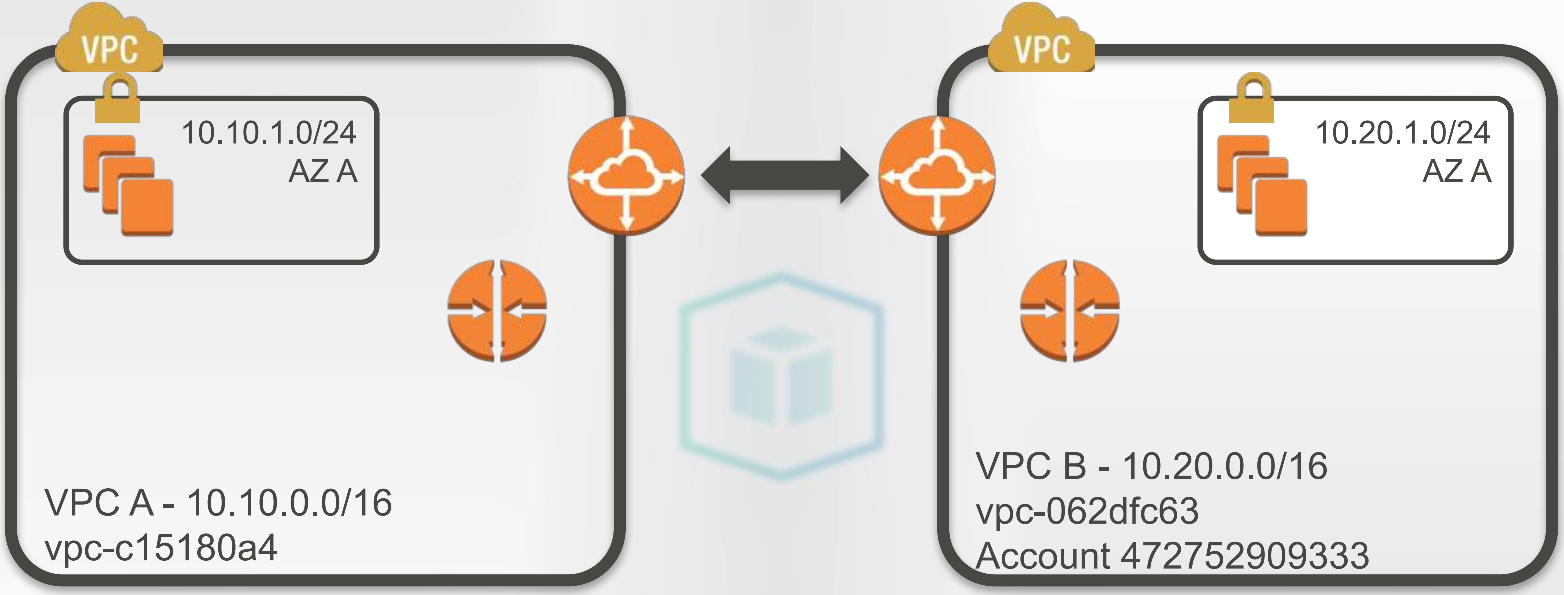
10.20.1.0/24
AZ A

VPC A - 10.10.0.0/16
vpc-c15180a4

VPC B - 10.20.0.0/16
vpc-062dfc63

```
aws ec2 create-vpc-peering-connection --vpc-id vpc-c15180a4 --peer-vpc vpc-062dfc63
aws ec2 accept-vpc-peering-connection --vpc-peer pcx-ee56be87
VPC A> aws ec2 create-route --ro rtb-ef36e58a --des 10.20.0.0/16 --vpc-peer pcx-ee56be87
VPC B> aws ec2 create-route --ro rtb-67a2b31c --des 10.10.0.0/16 --vpc-peer pcx-ee56be87
```

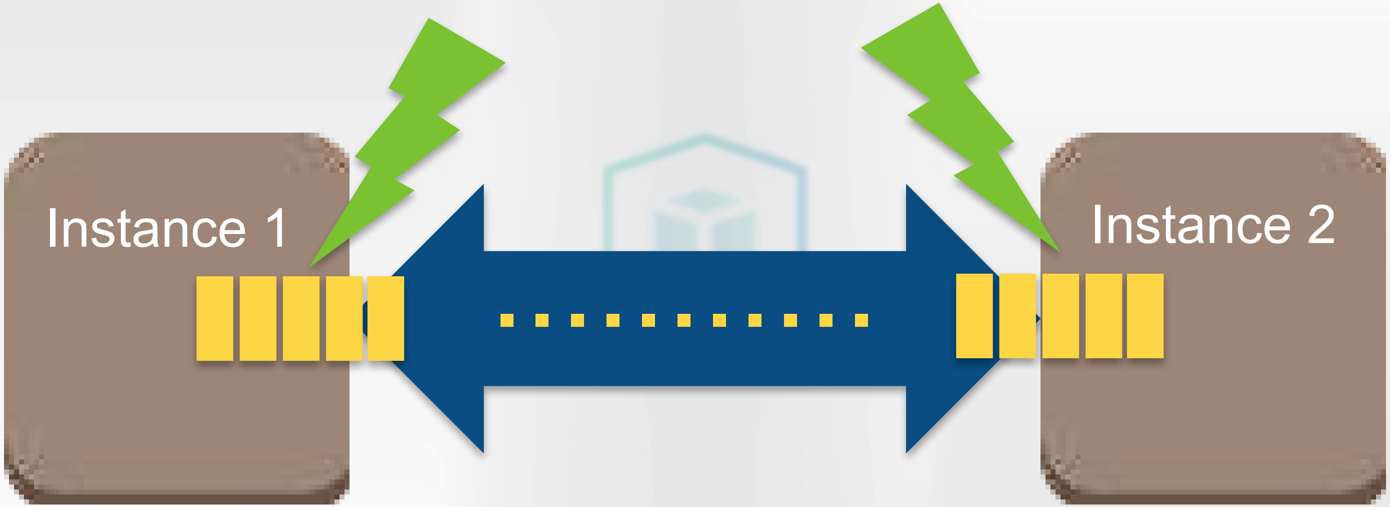
VPC peering in different accounts



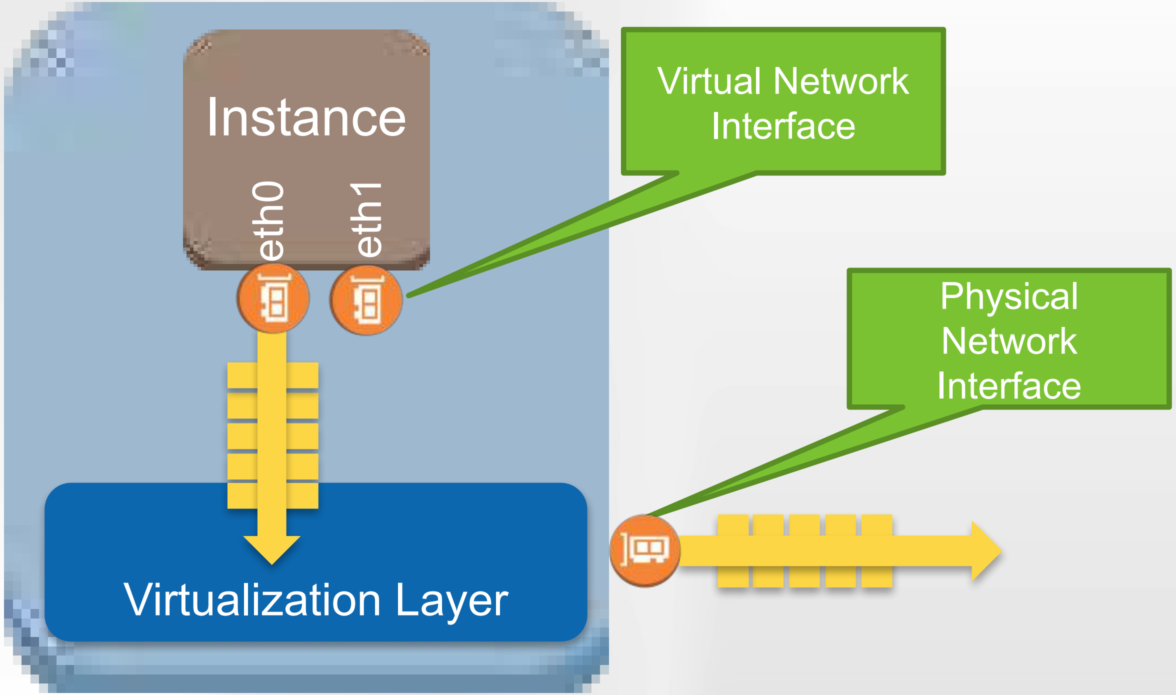
```
aws ec2 create-vpc-peering-connection --vpc-id vpc-c15180a4 --peer-vpc vpc-062dfc63
        --peer-owner 472752909333
# In account 472752909333
aws ec2 accept-vpc-peering-connection --vpc-peer pcx-ee56be87
```

Enhanced Networking

Latency: how many packets per second?



Packet processing in Amazon EC2: VIF

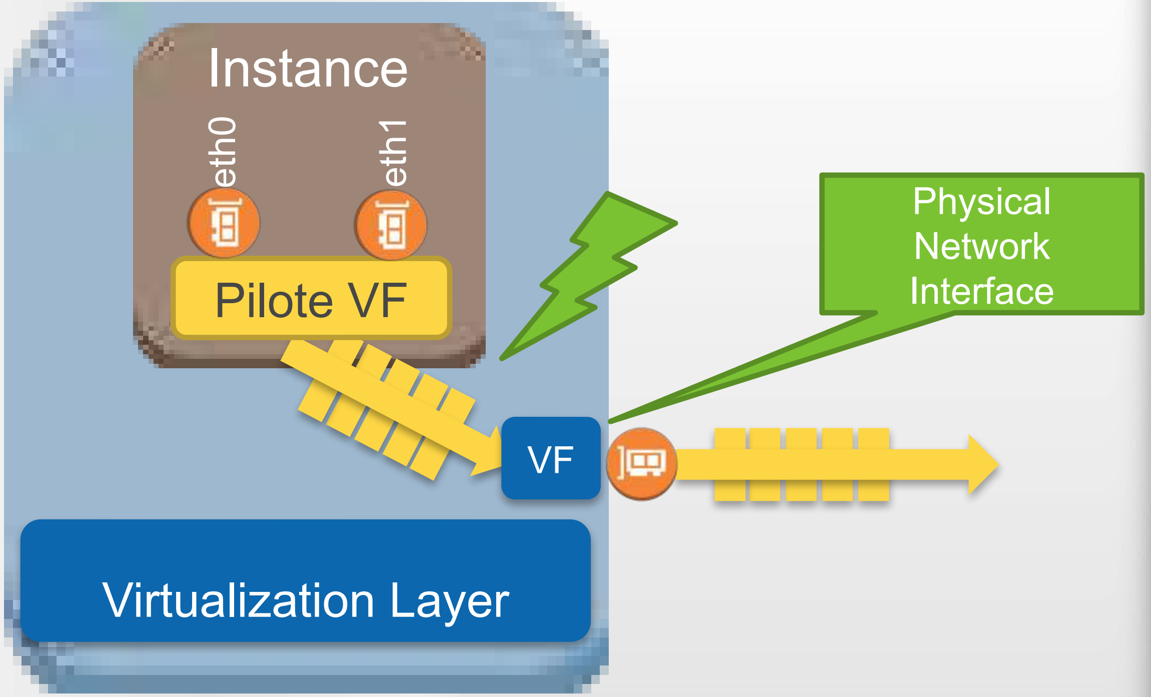


Packet processing in Amazon EC2: SRIOV

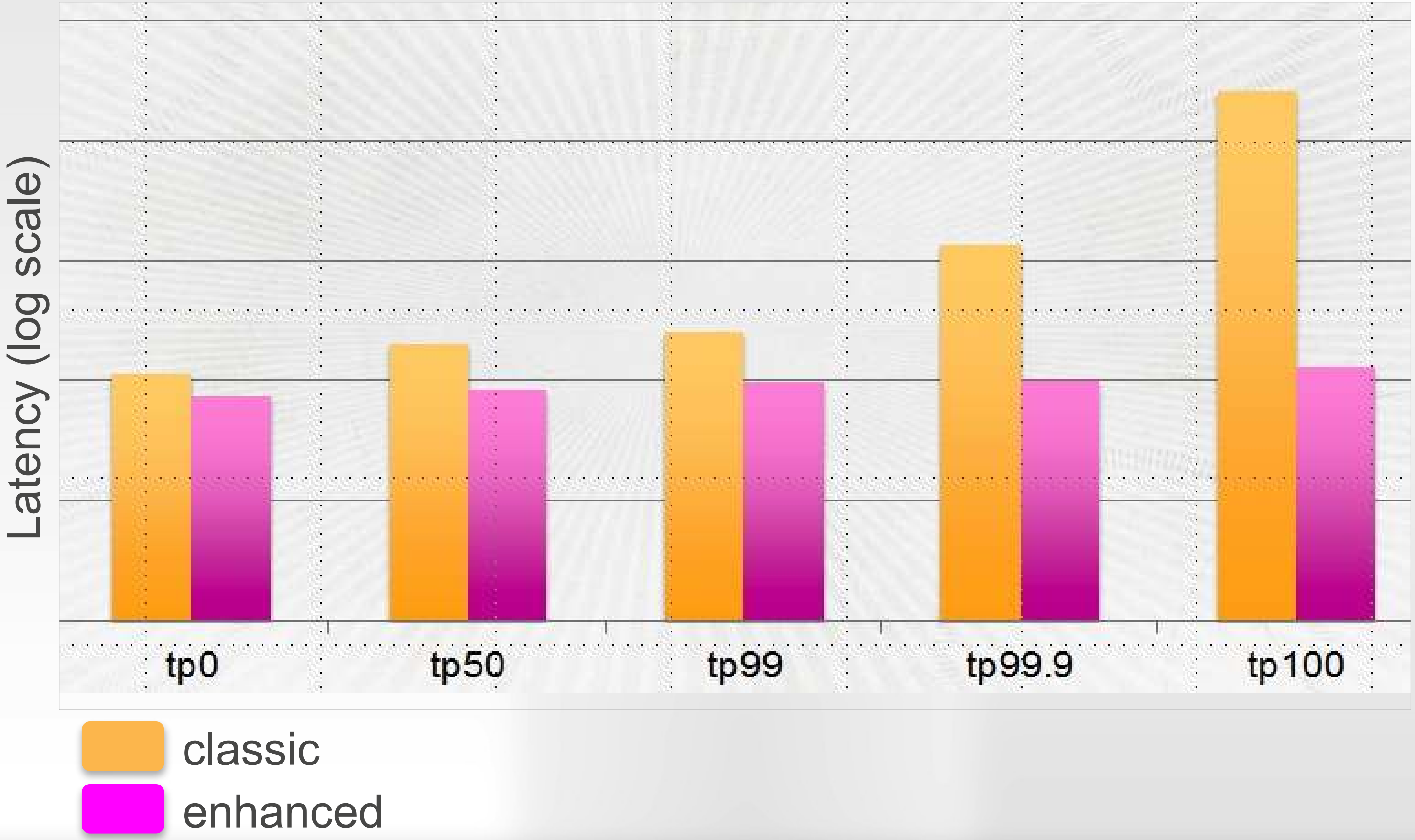
Packets do not go through the virtualization layer any more.

The network driver has direct access to the physical network interface.

This must be configured on your instance



Latency across instances



SRIOV: can I use it?

On recent AMIs, Enhanced Networking is enabled by default

- AMI Amazon Linux
- AMI Windows Server 2012 R2

No configuration necessary

SRIOV: Linux

No

```
[ec2-user@ip-10-0-3-70 ~]
$ ethtool -i eth0

driver: vif
version:
firmware-version:
bus-info: vif-0
…
```

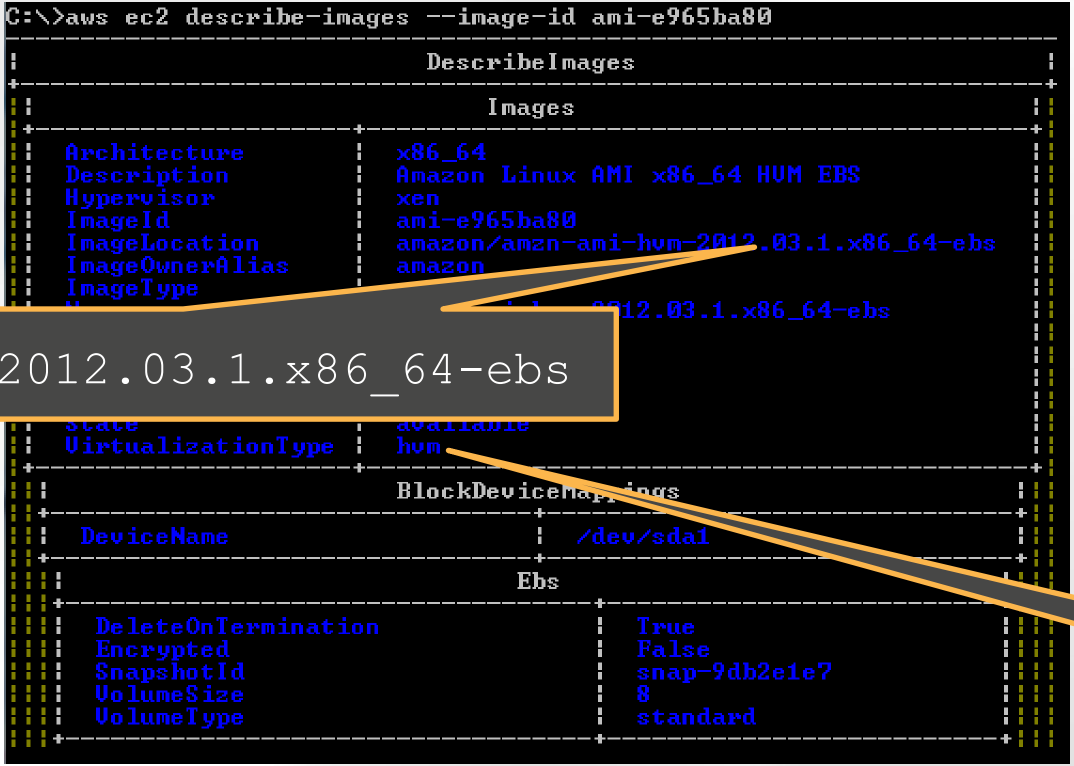
Yes!

```
[ec2-user@ip-10-0-3-70 ~]$
ethtool -i eth0

driver: ixgbevf
version: 2.14.2+amzn
firmware-version: N/A
bus-info: 0000:00:03.0
…
```

SRIOV support

- Instance families
  C3, C4, I2, I3, D2, R3, R4, M4, P2, X1
- HVM virtualization
- OS version
  - Linux : >= 2.6.32
  - Windows : >= Server 2008 R2
- VF driver
  - Linux : module ixgbevf 2.14.2+
  - Windows : Intel® 82599 driver

Enable *Enhanced Networking* (Amazon Linux)



```
C:\>aws ec2 describe-images --image-id ami-e965ba80
-------------------------------------------------------------------------
|                            DescribeImages                             |
+-----------------------------------------------------------------------+
||                               Images                                ||
|+-----------------------+---------------------------------------------+|
||  Architecture         |  x86_64                                     ||
||  Description          |  Amazon Linux AMI x86_64 HVM EBS            ||
||  Hypervisor           |  xen                                        ||
||  ImageId              |  ami-e965ba80                               ||
||  ImageLocation        |  amazon/amzn-ami-hvm-2012.03.1.x86_64-ebs   ||
||  ImageOwnerAlias      |  amazon                                     ||
||  ImageType            |                                             ||
||                                    012.03.1.x86_64-ebs              ||
||  State                |  available                                  ||
||  VirtualizationType   |  hvm                                        ||
|+-----------------------+---------------------------------------------+|
|||                        BlockDeviceMappings                        |||
||+----------------------------------+--------------------------------+||
|||  DeviceName                      |  /dev/sda1                     |||
||+----------------------------------+--------------------------------+||
||||                                Ebs                              ||||
|||+-----------------------------------+-----------------------------+|||
||||  DeleteOnTermination              |  True                       ||||
||||  Encrypted                        |  False                      ||||
||||  SnapshotId                       |  snap-9db2e1e7              ||||
||||  VolumeSize                       |  8                          ||||
||||  VolumeType                       |  standard                   ||||
|||+-----------------------------------+-----------------------------+|||
```

amzn-ami-hvm-2012.03.1.x86_64-ebs

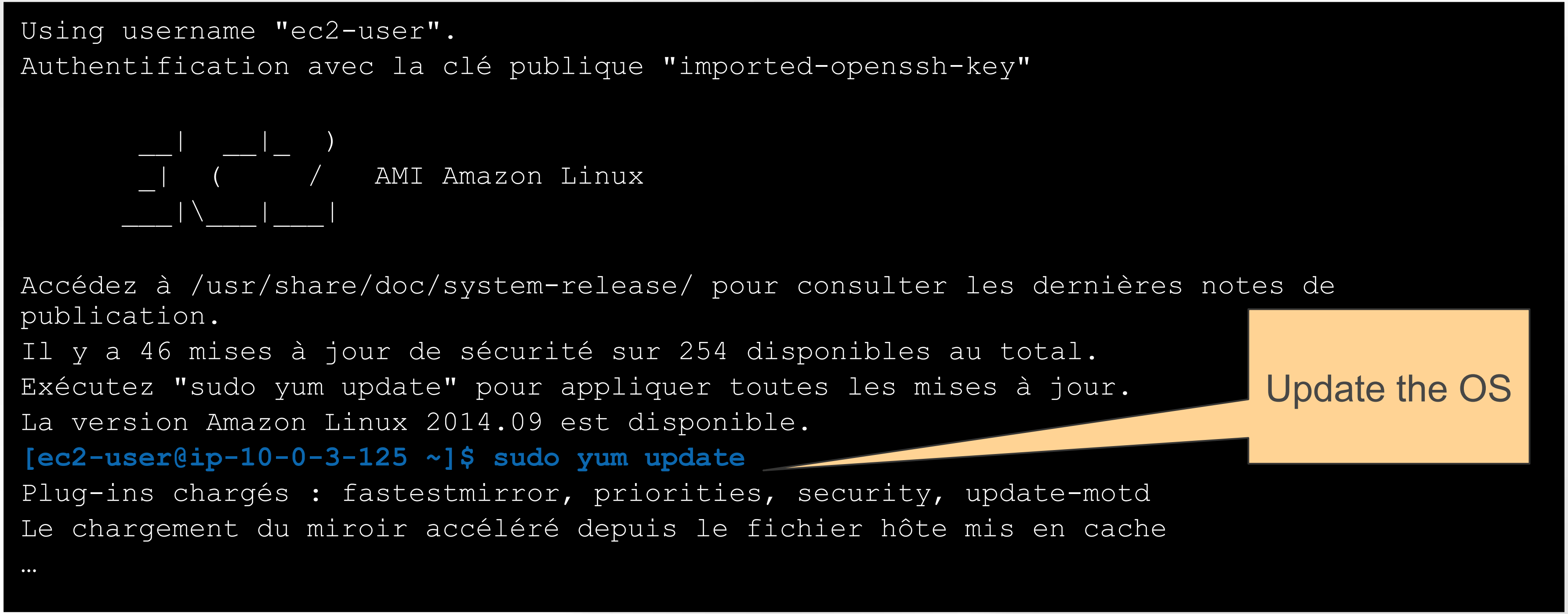
hvm

Enable *Enhanced Networking* (Amazon Linux)

```
C:\>aws ec2 describe-instance-attribute --
instance-id i-37c5d1d9 --attribute
sriovNetSupport
------------------------------

|   DescribeInstanceAttribute |

+-------------+----------------+

|  InstanceId |  i-37c5d1d9    |

+-------------+----------------+
```

Not yet

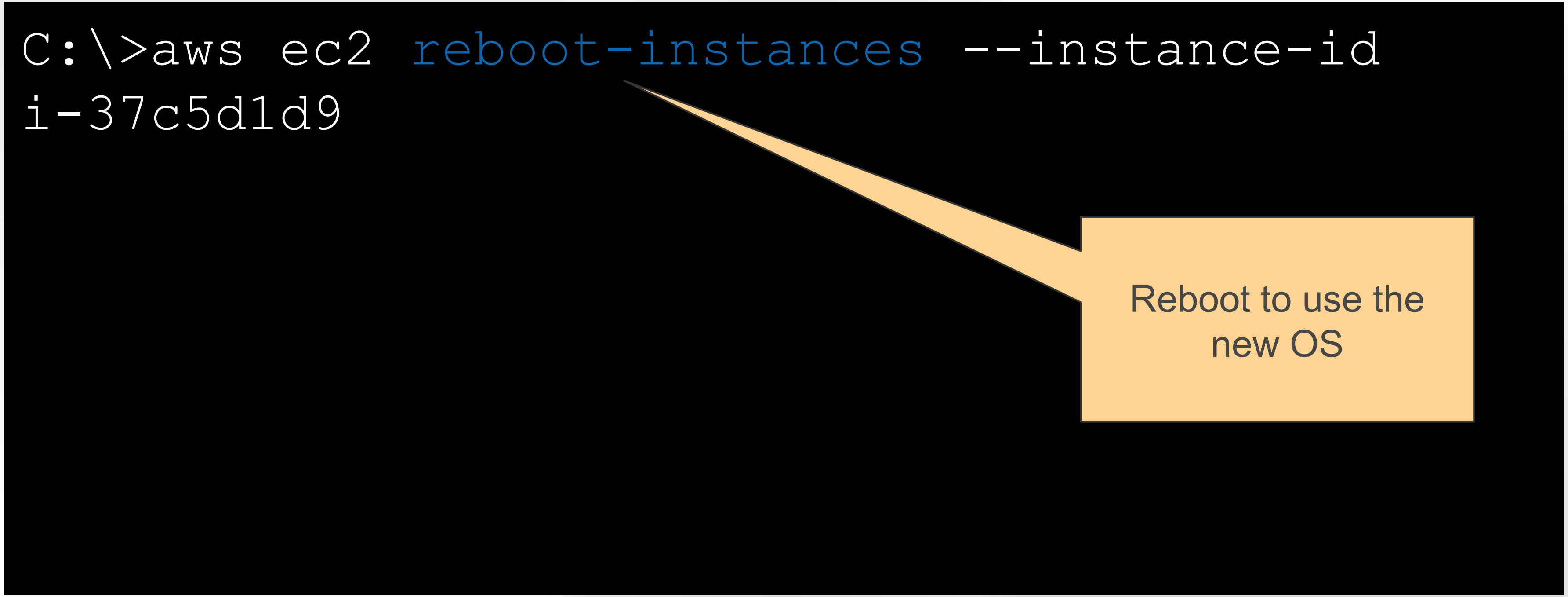
Enable *Enhanced Networking* (Amazon Linux)



```
Using username "ec2-user".
Authentification avec la clé publique "imported-openssh-key"

       __|  __|_  )
       _|  (     /   AMI Amazon Linux
      ___|\___|___|

Accédez à /usr/share/doc/system-release/ pour consulter les dernières notes de
publication.
Il y a 46 mises à jour de sécurité sur 254 disponibles au total.
Exécutez "sudo yum update" pour appliquer toutes les mises à jour.
La version Amazon Linux 2014.09 est disponible.
[ec2-user@ip-10-0-3-125 ~]$ sudo yum update
Plug-ins chargés : fastestmirror, priorities, security, update-motd
Le chargement du miroir accéléré depuis le fichier hôte mis en cache
…
```

Update the OS

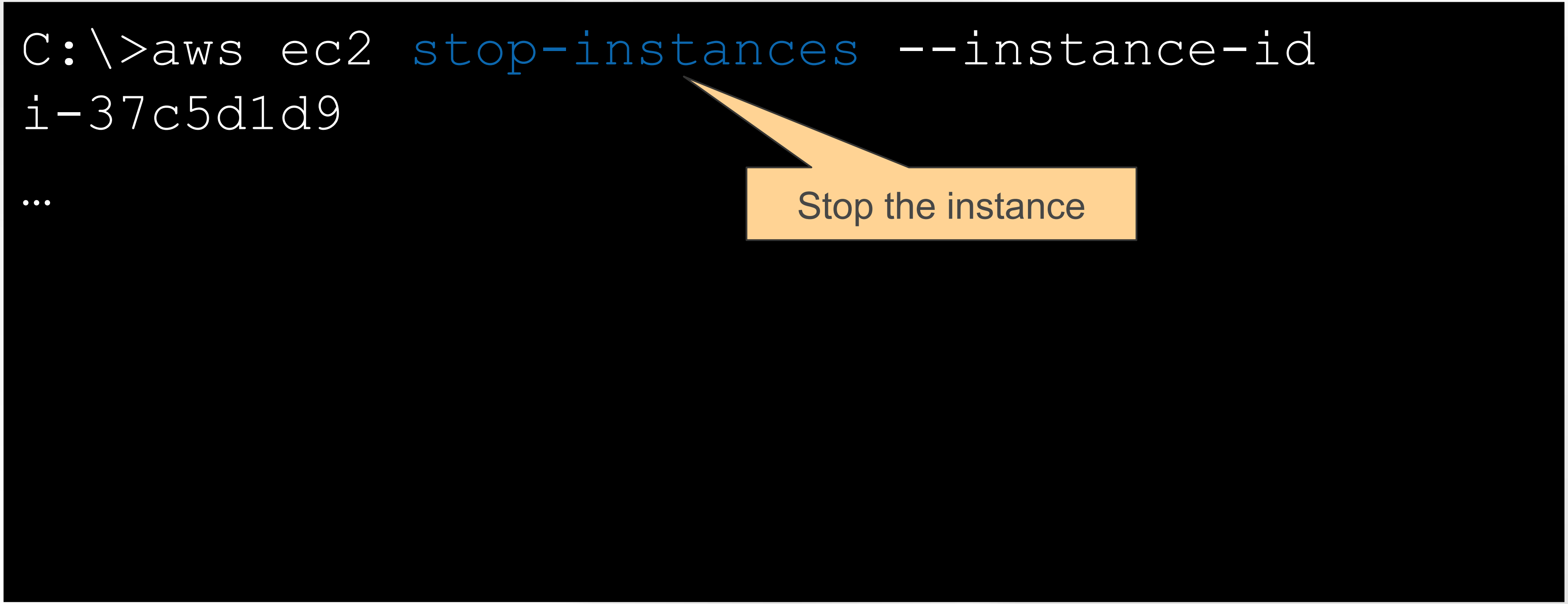
Enable *Enhanced Networking* (Amazon Linux)



```
C:\>aws ec2 reboot-instances --instance-id
i-37c5d1d9
```

Reboot to use the new OS

Enable *Enhanced Networking* (Amazon Linux)



```
C:\>aws ec2 stop-instances --instance-id
i-37c5d1d9

…
```

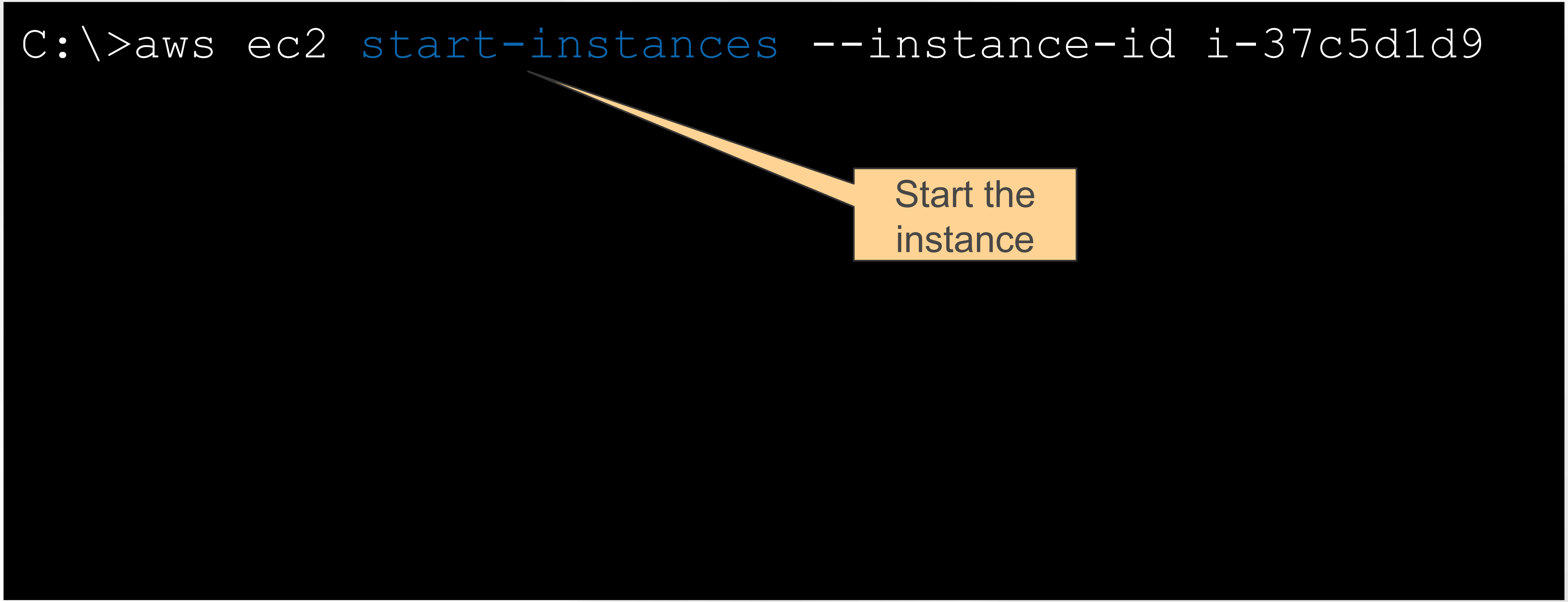
Stop the instance

Enable *Enhanced Networking* (Amazon Linux)

```
C:\>aws ec2 stop-instances --instance-id
i-37c5d1d9

…

C:\>aws ec2 modify-instance-attribute –
instance-id i-37c5d1d9 --sriov-net-support
simple
```

Enable SRIOV
(you can’t go back!)

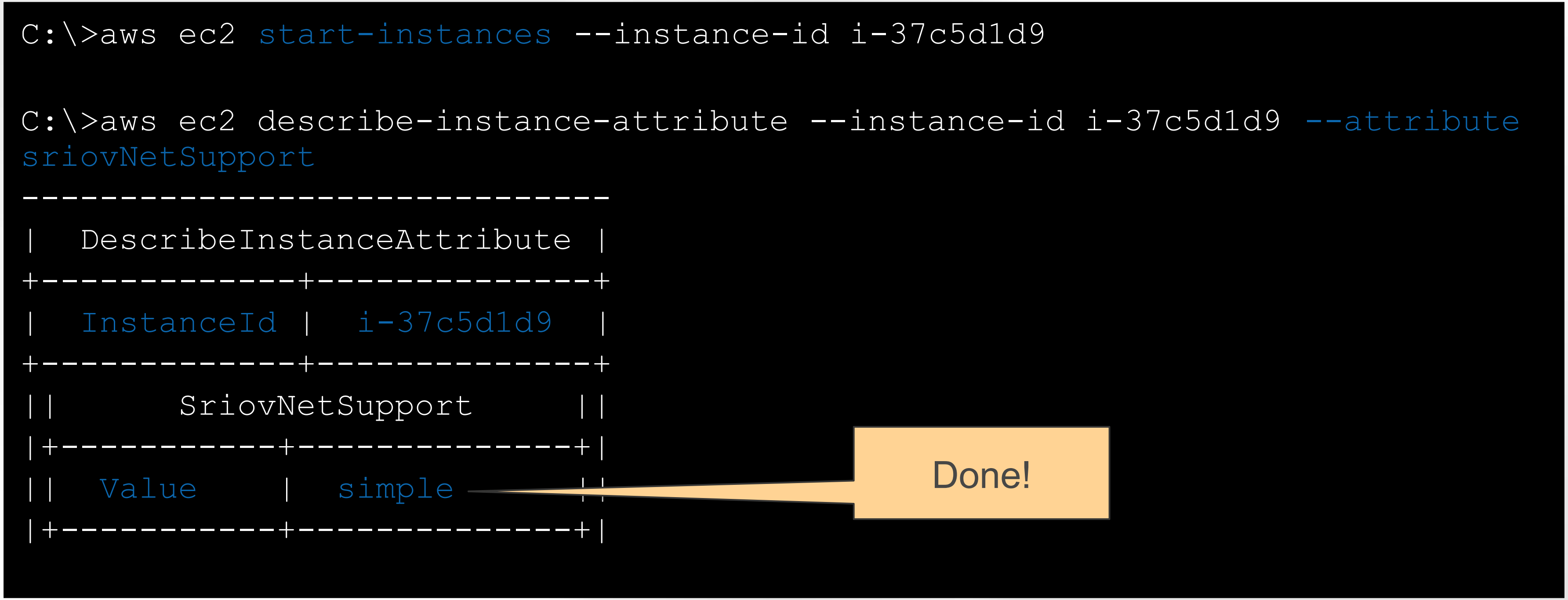
Enable *Enhanced Networking* (Amazon Linux)



```
C:\>aws ec2 start-instances --instance-id i-37c5d1d9
```

Start the instance

Enable *Enhanced Networking* (Amazon Linux)

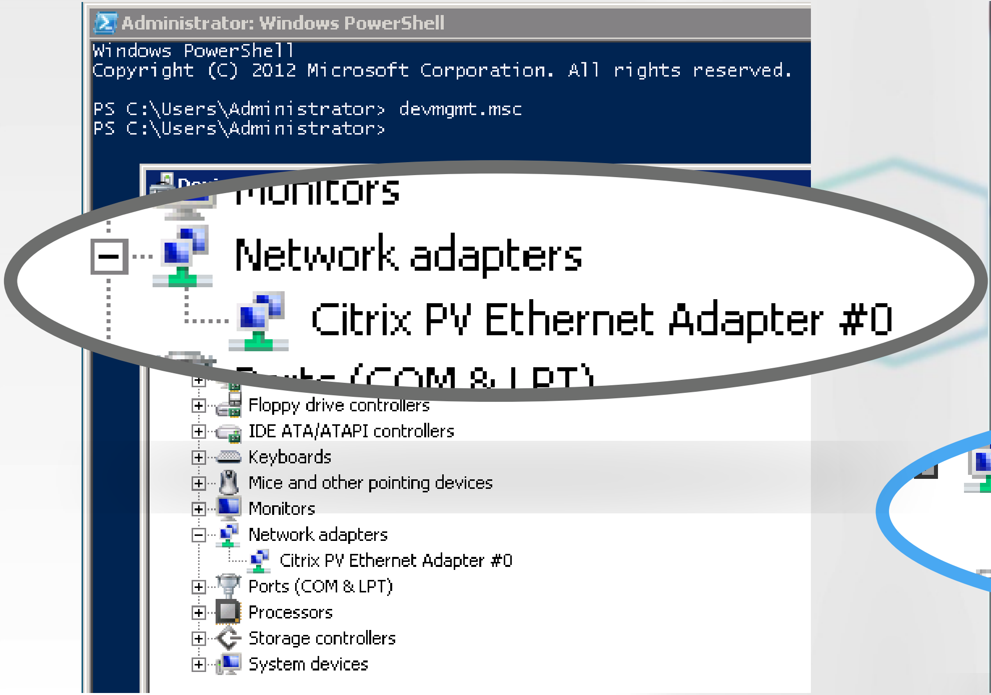


```
C:\>aws ec2 start-instances --instance-id i-37c5d1d9

C:\>aws ec2 describe-instance-attribute --instance-id i-37c5d1d9 --attribute
sriovNetSupport
------------------------------
|  DescribeInstanceAttribute |
+-------------+--------------+
|  InstanceId |  i-37c5d1d9  |
+-------------+--------------+
||      SriovNetSupport     ||
|+-----------+--------------+|
||  Value    |  simple      ||
|+-----------+--------------+|
```

Done!

SRIOV: Windows

No

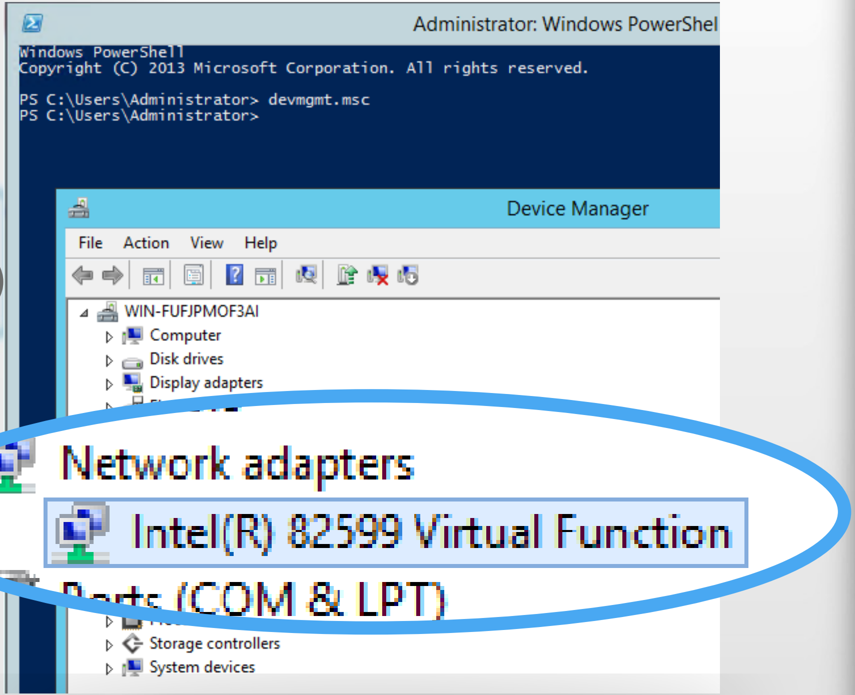


Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> devmgmt.msc
PS C:\Users\Administrator>
```

- Monitors
- Network adapters
  - Citrix PV Ethernet Adapter #0
- Ports (COM & LPT)
- Floppy drive controllers
- IDE ATA/ATAPI controllers
- Keyboards
- Mice and other pointing devices
- Monitors
- Network adapters
  - Citrix PV Ethernet Adapter #0
- Ports (COM & LPT)
- Processors
- Storage controllers
- System devices

Yes !



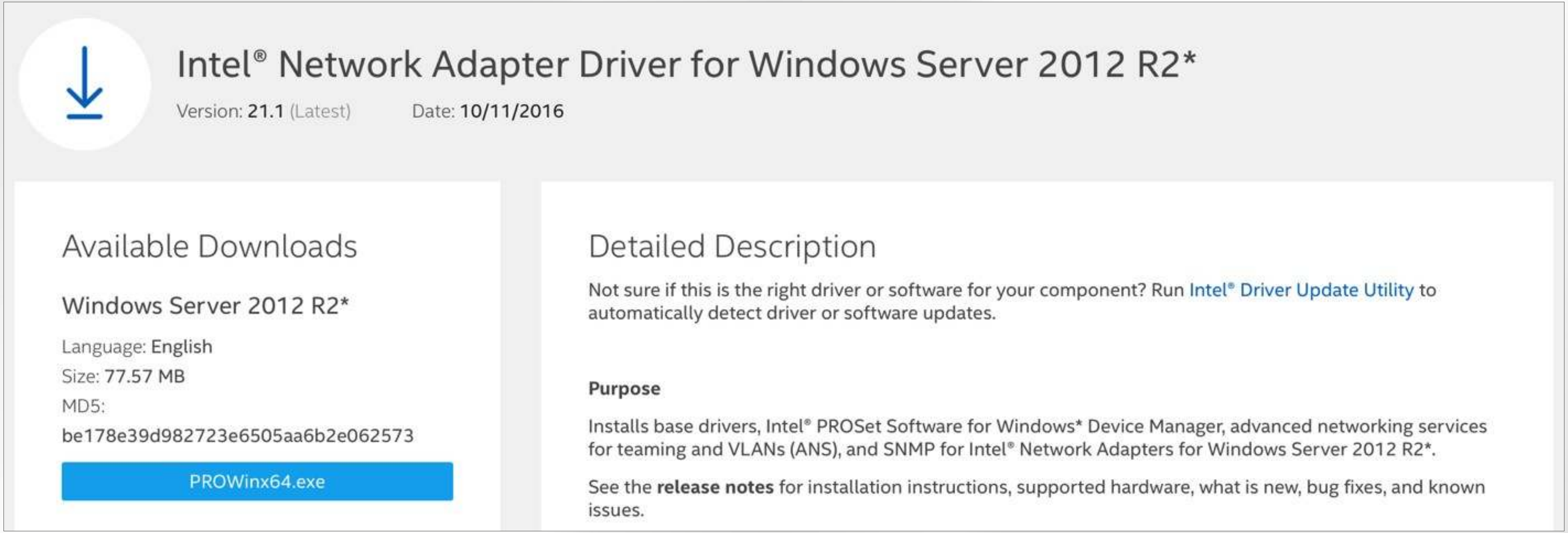
Administrator: Windows PowerShel

```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> devmgmt.msc
PS C:\Users\Administrator>
```

Device Manager

- WIN-FUFJPMOF3AI
  - Computer
  - Disk drives
  - Display adapters
  - Network adapters
    - Intel(R) 82599 Virtual Function
  - Ports (COM & LPT)
  - Storage controllers
  - System devices

Enable *Enhanced Networking* (Windows)



Intel® Network Adapter Driver for Windows Server 2012 R2*

Version: 21.1 (Latest) Date: 10/11/2016

Available Downloads

Windows Server 2012 R2*

Language: English

Size: 77.57 MB

MD5:
be178e39d982723e6505aa6b2e062573

Detailed Description

Not sure if this is the right driver or software for your component? Run Intel® Driver Update Utility to automatically detect driver or software updates.

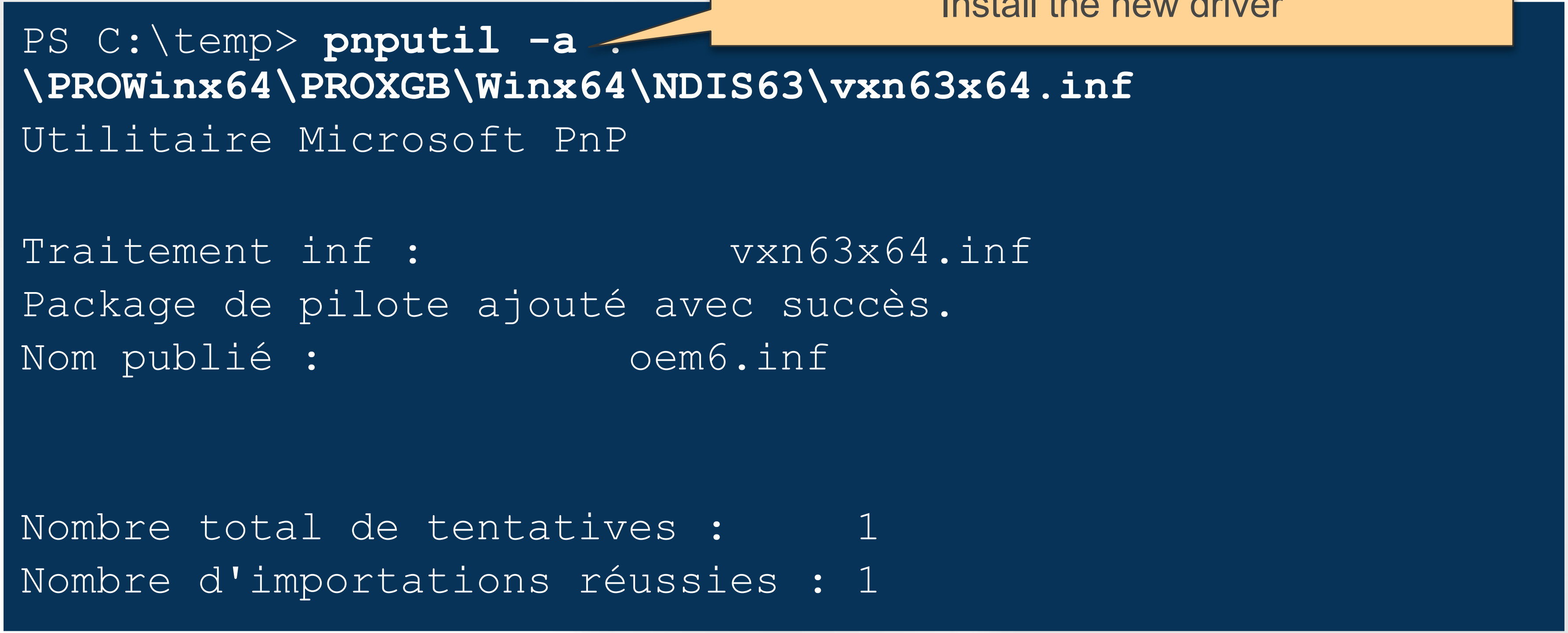
Purpose

Installs base drivers, Intel® PROSet Software for Windows* Device Manager, advanced networking services for teaming and VLANs (ANS), and SNMP for Intel® Network Adapters for Windows Server 2012 R2*.

See the **release notes** for installation instructions, supported hardware, what is new, bug fixes, and known issues.

http://docs.aws.amazon.com/fr_fr/AWSEC2/latest/WindowsGuide/sriov-networking.html

Enable *Enhanced Networking* (Windows)



Install the new driver

```
PS C:\temp> pnputil -a .
\PROWinx64\PROXGB\Winx64\NDIS63\vxn63x64.inf
Utilitaire Microsoft PnP

Traitement inf :            vxn63x64.inf
Package de pilote ajouté avec succès.
Nom publié :            oem6.inf



Nombre total de tentatives :     1
Nombre d'importations réussies : 1
```

TIRED.
JUST TIRED.
quickmeme.com

Additional Resources

AWS re:Invent 2016: Tuesday Night Live with James Hamilton
https://www.youtube.com/watch?v=AyOAjFNPAbA

AWS re:Invent 2016: Creating Your Virtual Data Center: VPC Fundamentals and Connectivity (NET201)
https://www.youtube.com/watch?v=Ul2NsPNh9Ik

AWS re:Invent 2016: NEW LAUNCH IPv6 in the Cloud: Protocol and AWS Service Overview (NET204)
https://www.youtube.com/watch?v=Uvgyxncu9MY

AWS re:Invent 2016: NextGen Networking: New Capabilities for Amazon's Virtual Private Cloud (NET303)
https://www.youtube.com/watch?v=G24h4PuAOrs

AWS re:Invent 2016: Extending Datacenters to the Cloud (NET305)
https://www.youtube.com/watch?v=F2AWkGem7Sw

AWS re:Invent 2016: Another Day, Another Billion Packets (NET401)
https://www.youtube.com/watch?v=St3SE4LWhKo

AWS re:Invent 2016: Deep Dive: AWS Direct Connect and VPNs (NET402)
https://www.youtube.com/watch?v=Qep11X1r1QA

Thank You

Julien Simon
julsimon@amazon.fr
@julsimon

Your feedback is important to us!

amazon web services | Pop-up Loft TEL AVIV