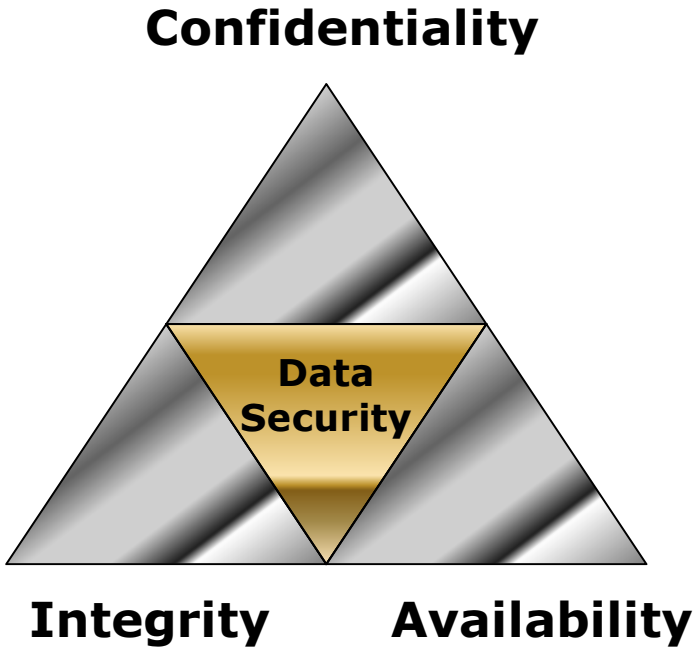
CERTES NETWORKS

Did you solve all your e-Crime problems before moving to cloud?

Istanbul, April 2012

Franjo Majstor
Sr. Technical Director - EMEA
Certes Networks Inc.
franjo@certesnetworks.com

Think CIA for Complete Security



- **Confidentiality - Render data unreadable/unusable to unauthorized parties**
- **Integrity - Prevent/detect when data has been altered**
- **Availability- Don't interrupt data flows - don't give the bad guys "air cover"**

Performance trumps Security

Security is important - but you still can't "mess up" the business applications or access to the network

Router based solutions ALWAYS performance!

- **The CPU can only do much**
- **Forces a premature upgrade, or decreased performance**
- **Often requires "work-arounds"**

Go Beyond Compliance

You can be compliant
and still not be secure.

If you are secure,
you are almost always compliant

Applying Security Best Practices

- Fixes the primary problem (Risk of data theft/loss)
- Fixes the secondary problem (compliance) by default
- Helps mitigate the tertiary problem (costs of audits)

Least Privilege and Separation of Duties

Least Privilege: Give users only those privileges which are absolutely required to perform their jobs

Separation of duties: Divide tasks so that one employee cannot create a security breach through negligence or malicious intent

"There needs to be a clear delineation between networking and security because the groups' focuses and goals are different."

"Simply put, the networking group should maintain and configure network devices, and the security group should maintain and configure security devices"

Shon Harris - author of the study guides for the CISSP

Invest for the Long Haul

Networks are in a constant state of change

Transparency / Immunity

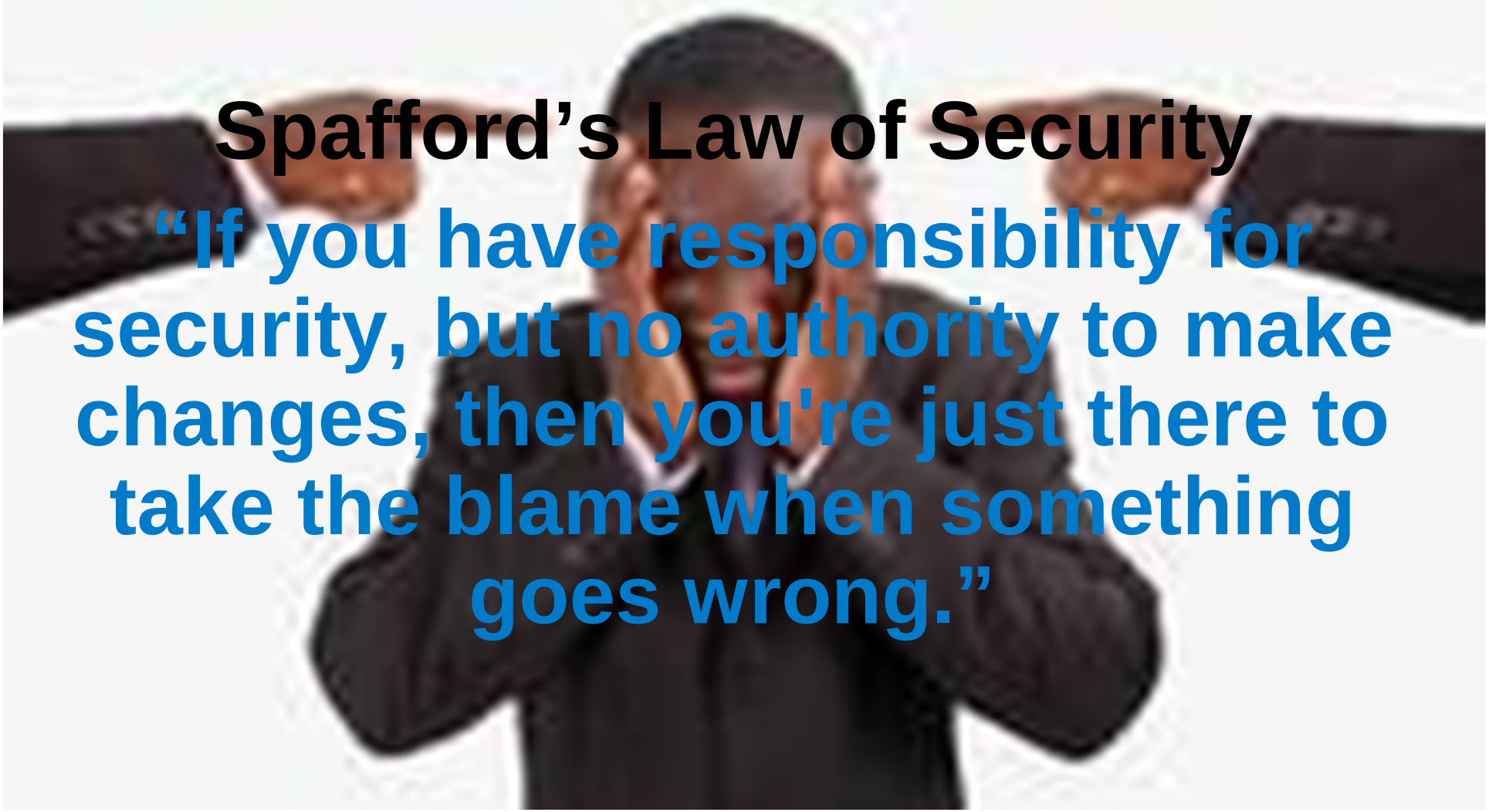
- **Solutions that can "absorb" or be immune to these changes are of higher value than those that can't**

Flexibility

- **If changes are unavoidable - pick a solution that can be easily re-configured**
- **When security is decoupled from the infrastructure allows infrastructure to stay in place longer and perform better**

The ideal is to provide "stable security" in an ever-changing world

If you own it - control it



Spafford's Law of Security

"If you have responsibility for security, but no authority to make changes, then you're just there to take the blame when something goes wrong."

Private Residence

Hotel

Youth Hostel

Infrastructure Options

Data Center

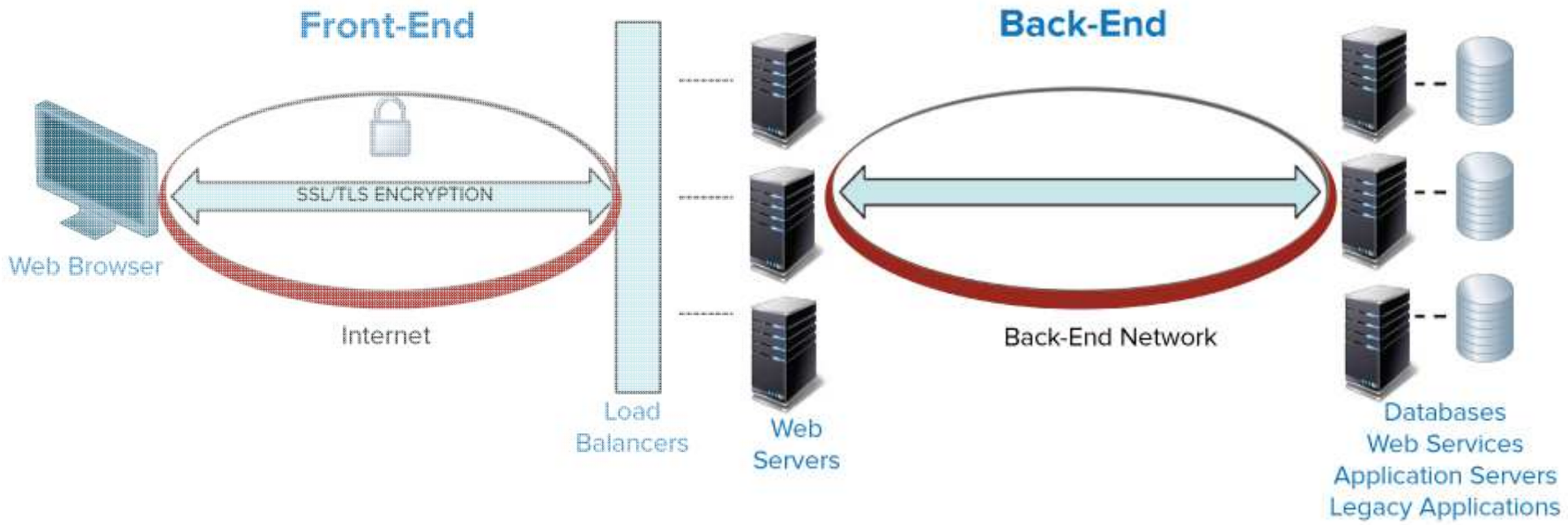
Public cloud

Secure Public Cloud

- **Private**
- **Shared**
- **Secure**
- **Cost effective**

- ***Reduce data center costs by 75-85%***
- ***Do it securely in a phased approach***

Front-End vs. Back-End Networks



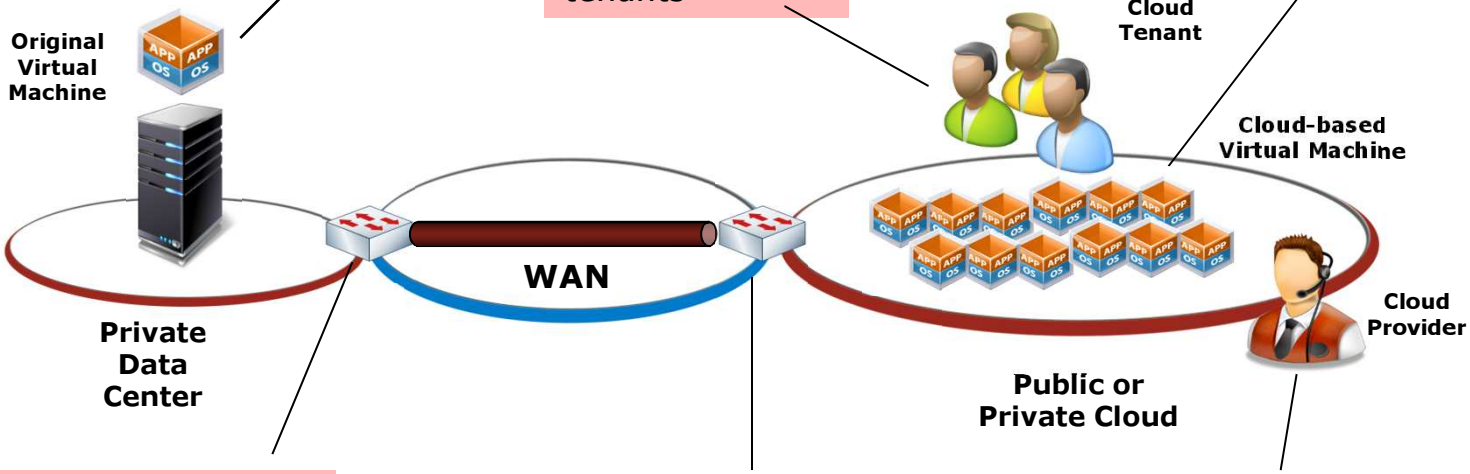
How to encrypt the Back-end network in a cloud environment?

Cloud Security Issues

Existing virtual machines require changes when moving to the cloud

There is no isolation between tenants

Tunnel based encryption solutions do not scale to 10's of thousands of VMs



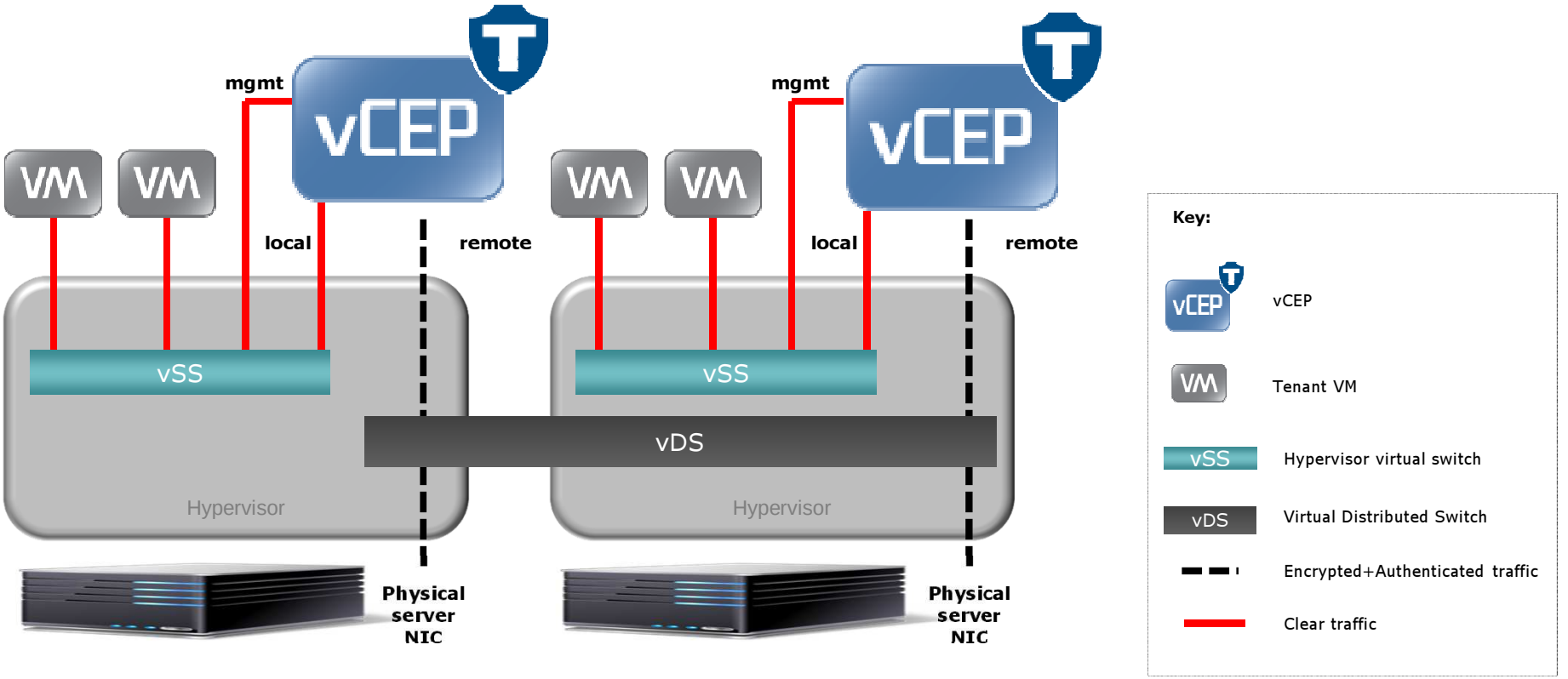
10 Gbps encryptors are not widely available, but are essential for large Data Centers

Many tunnel based encryption solutions stop at the provider's front door and leave the data exposed within the cloud

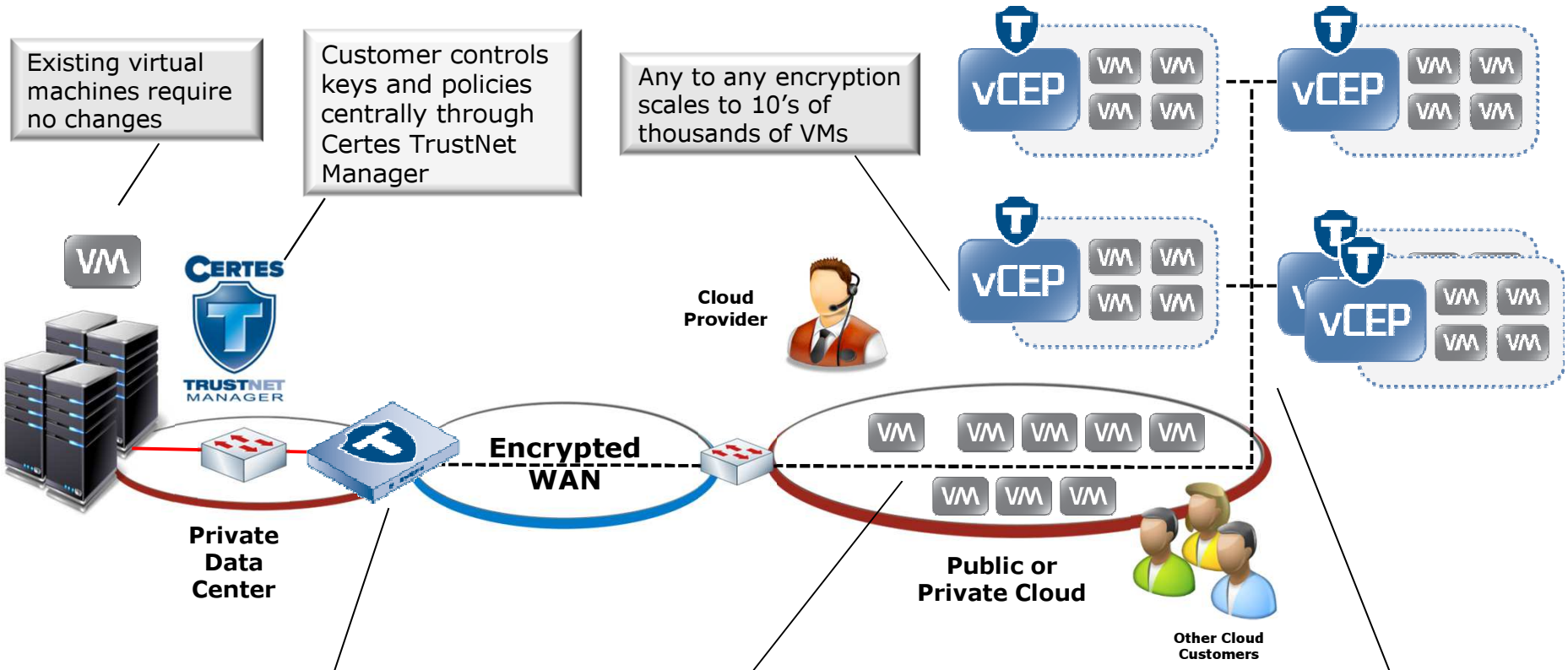
The cloud provider controls the encryption keys and policies

Virtual Encryption Concept

- Local and management ports – similar to vSS
- Remote port of the vCEP connects to vDS to provide distributed switching capability
- All VM traffic traverses and is protected by the virtual encryption appliance

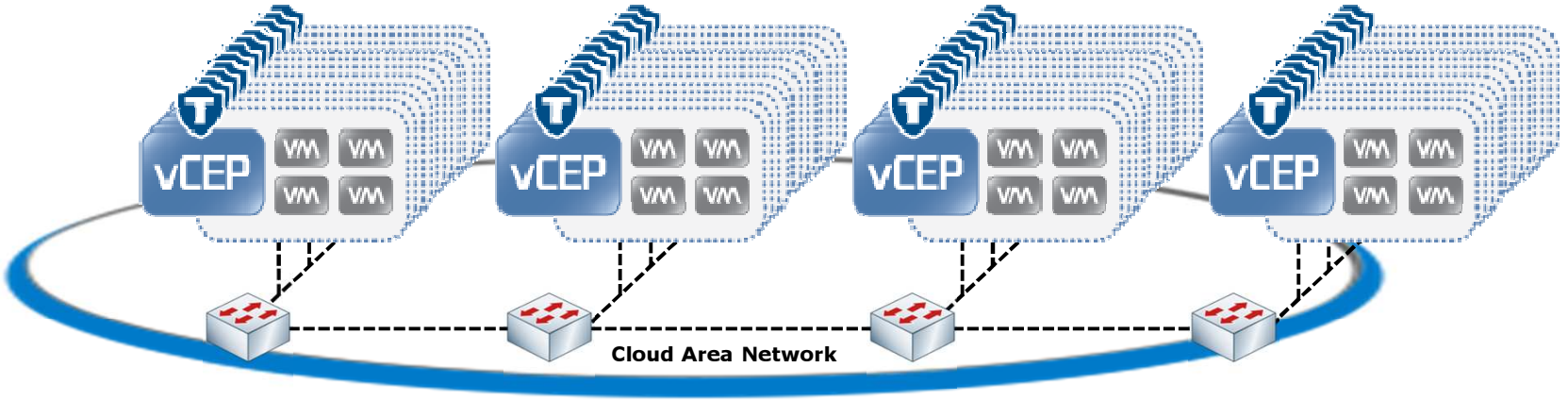


Cloud Security with encryption solution



Encryption Use Case: IaaS Cloud

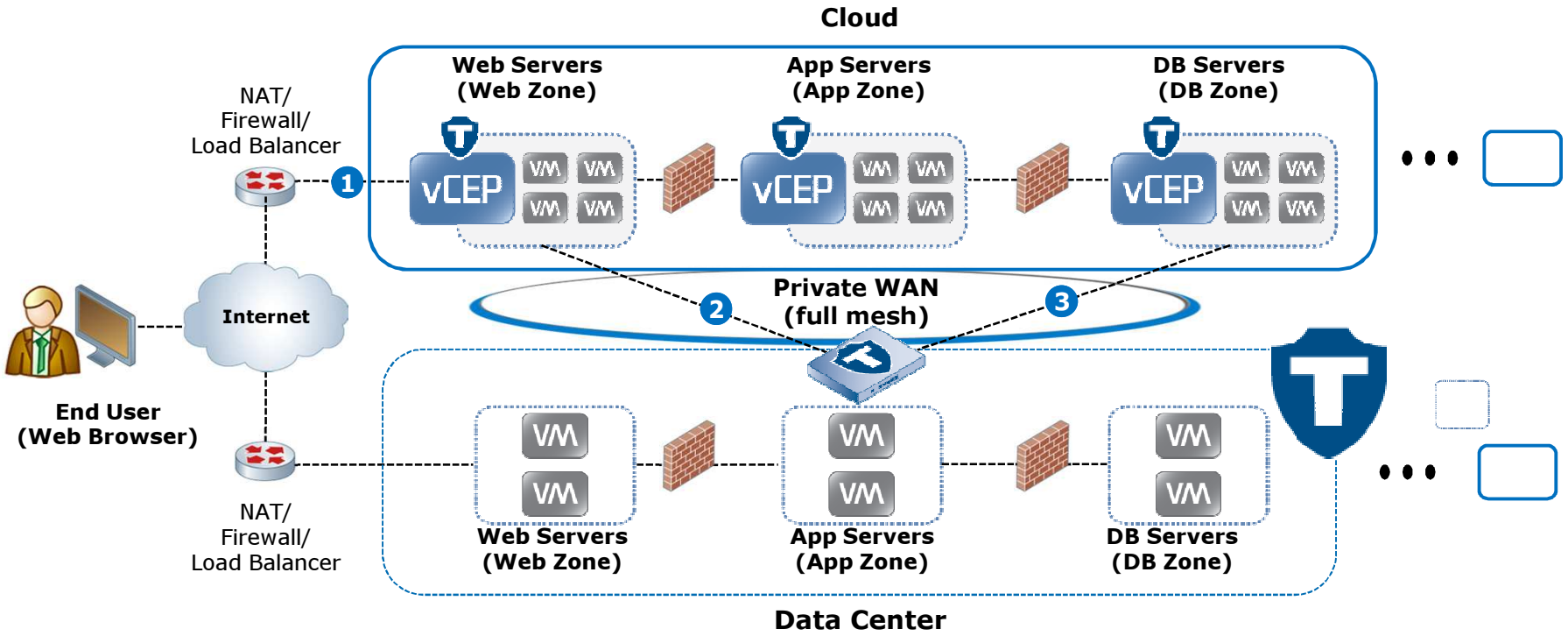
- Protect sensitive traffic among virtual servers in a cloud or shared virtualized environment
  - Offered by the IaaS provider or as a service by a 3rd party



Encryption Use Case: Crypto Segmentation

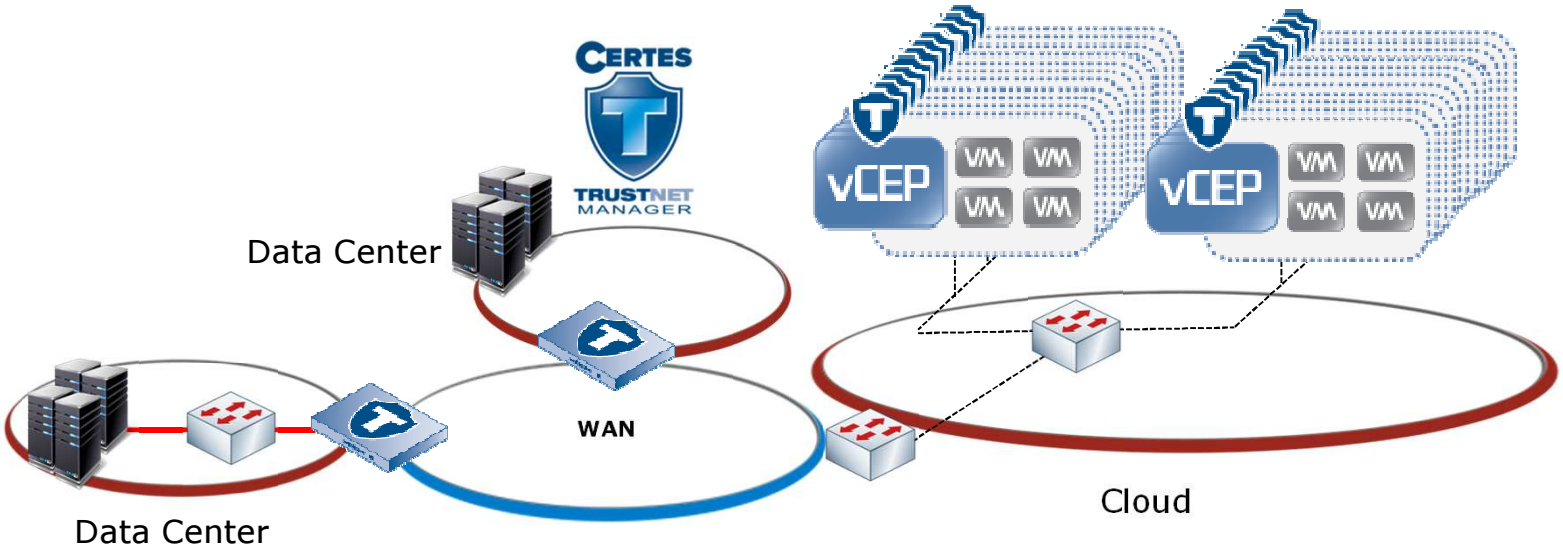
- Segment and encrypt among security zones (web, application and DB) in multiple sites
- Protect the Back-End network (behind the Web Servers)

1 Web browser connects to Web server (in the cloud) via SSL/TLS (encrypted)
2 Web server connects to App server (in the DC) protected by vCEP/CEP
3 App server connects to DB server (in the Cloud) protected by vCEP/CEP



Encryption Use Case: Cloud Migration

- Protect sensitive traffic among data centers and virtual servers in the cloud
- Full mesh connectivity among encryprtor and virtual encryptor



Cloud Security Alliance Recommendations

"…protect this sensitive and regulated information in transit even within the cloud provider's network."

"Segregate the key management from the cloud provider hosting the data, creating a chain of separation.

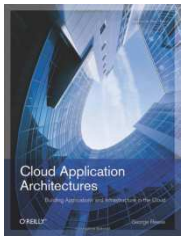
This protects both the cloud provider and tenant from conflicts when compelled to provide data due to a legal mandate."

"Understand whether and how cloud provider facilities provide role management and separation of duties"

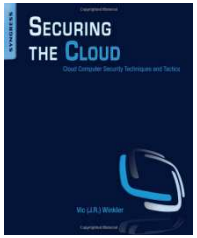
Security Guidance for Critical Areas of Focus in Cloud Computing V2.1

Recommended Reading

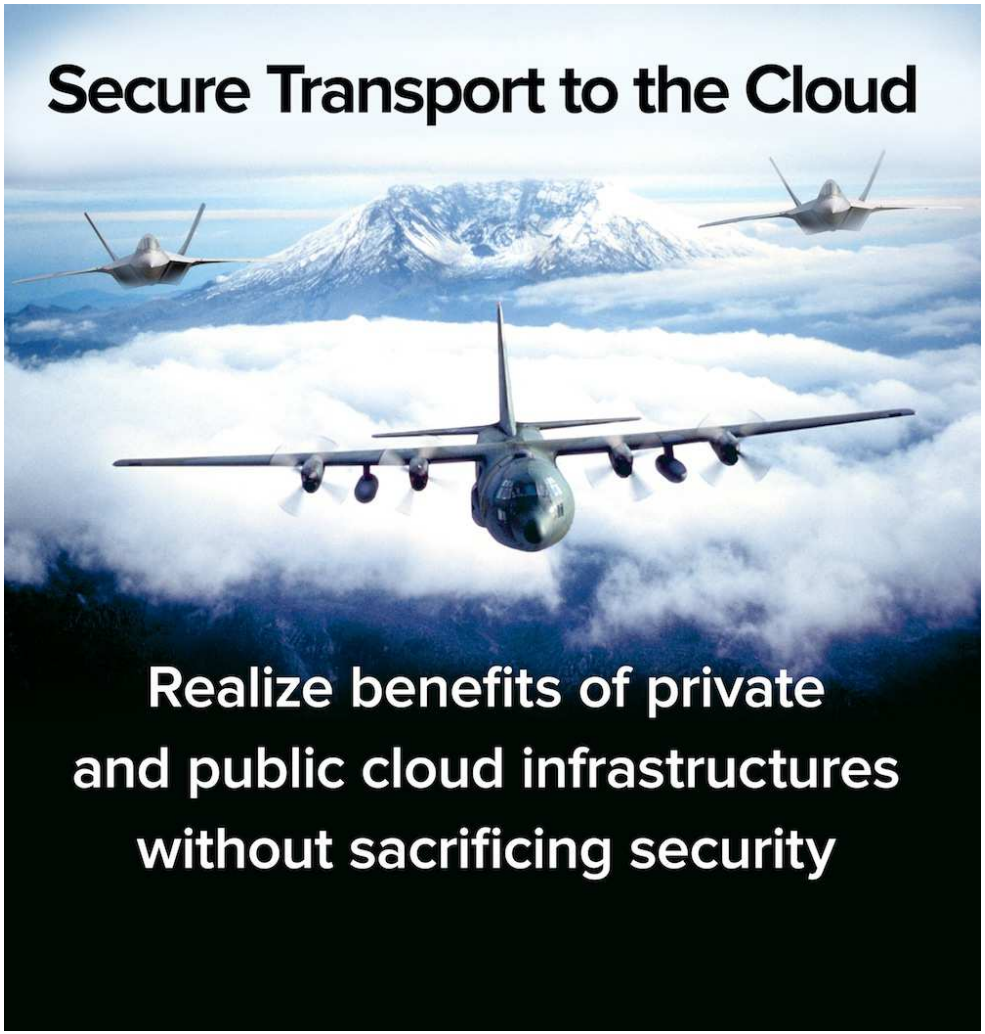
- VMWare documentation
  - http://www.vmware.com/support/pubs/
    - vSphere Networking Guide
    - vSphere Security Guide
    - vShield Design Guide
- Cloud Application Architectures
  - By George Reese



- Securing the Cloud
  - By Vic (J.R.) Winkler



Questions?


Secure Transport to the Cloud
Realize benefits of private
and public cloud infrastructures
without sacrificing security

CERTES NETWORKS

Thank you!