



IBM Research, Zurich Research Lab

# Towards Automated Provisioning of Secure Virtualized Networks

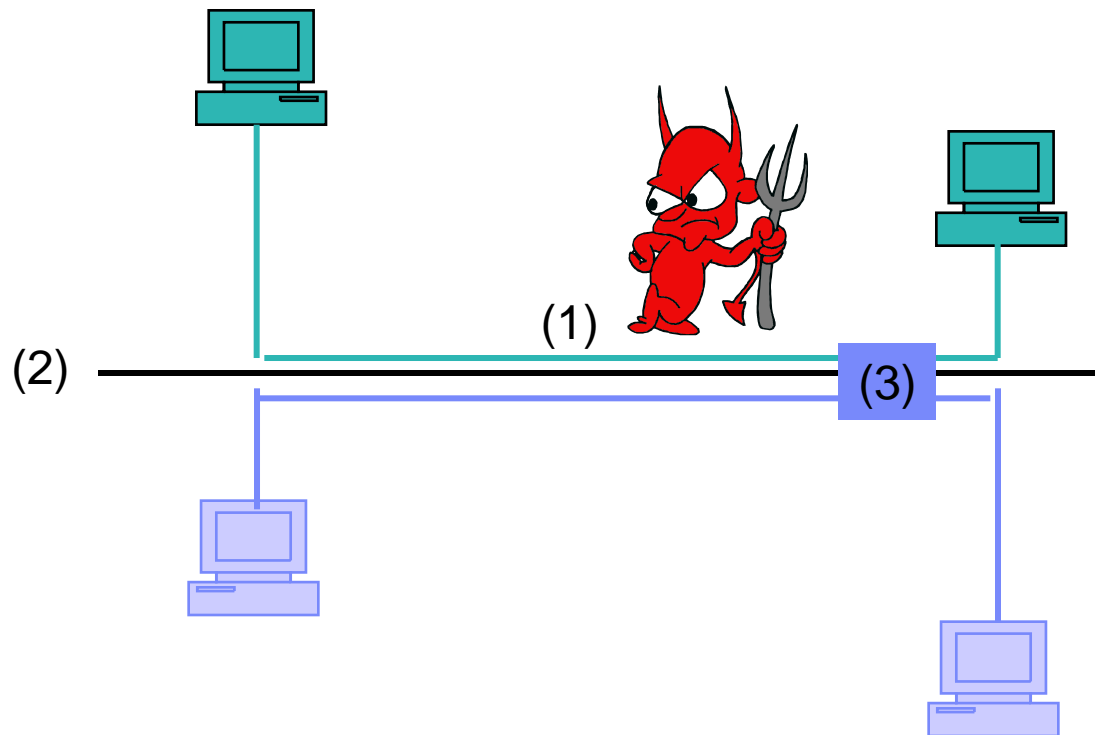
Serdar Cabuk, Chris I. Dalton

HP Labs, Bristol, UK

HariGovind Ramasamy, Matthias Schunter

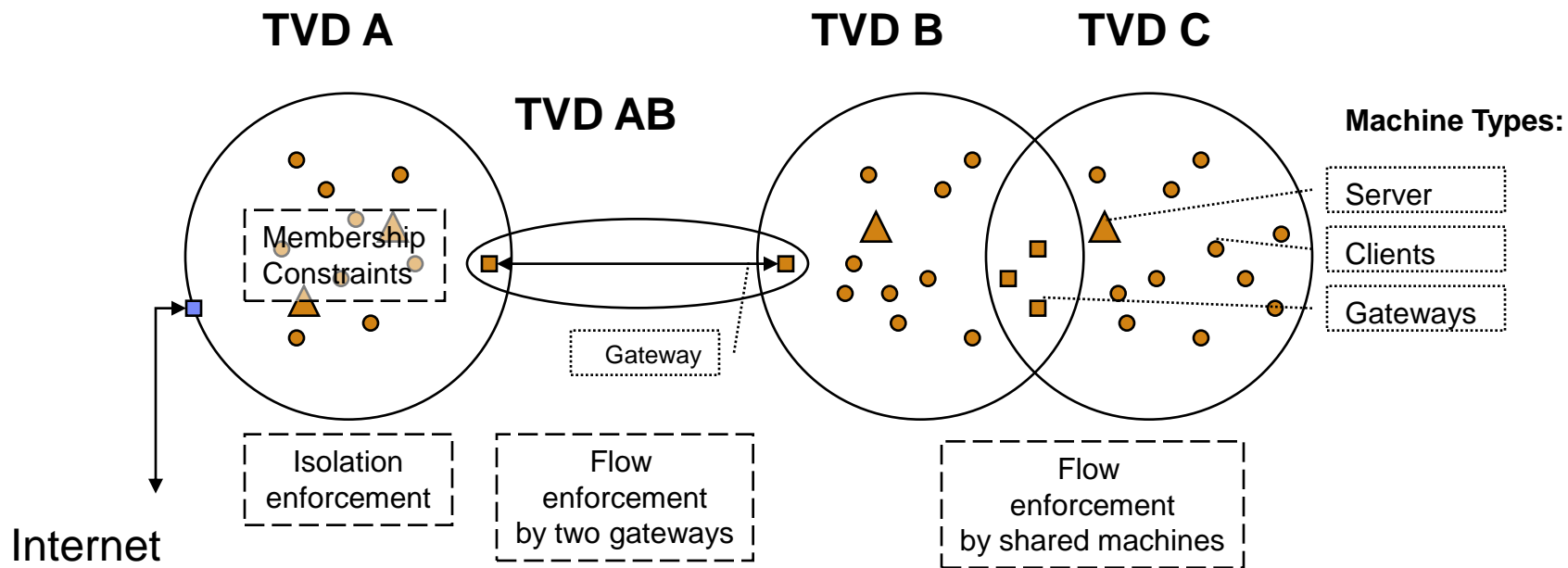
IBM Research, USA/Switzerland

# Virtual Datacenter Security: What do we want to achieve?



1. Security of each network despite attacks
2. Isolation between customers
3. Controlled flow between customers

Important: Do not rely on untrusted components



- **Domain Trusts certain components:**
  - Infrastructure Networks for Confidentiality/Integrity
  - Guards/gateways for Trust
- **Our approach:**
  - Bridge a security gap (trusted components <-> requirements)
- **Important: Shared trust vs. no shared trust**

# Flow control Policies

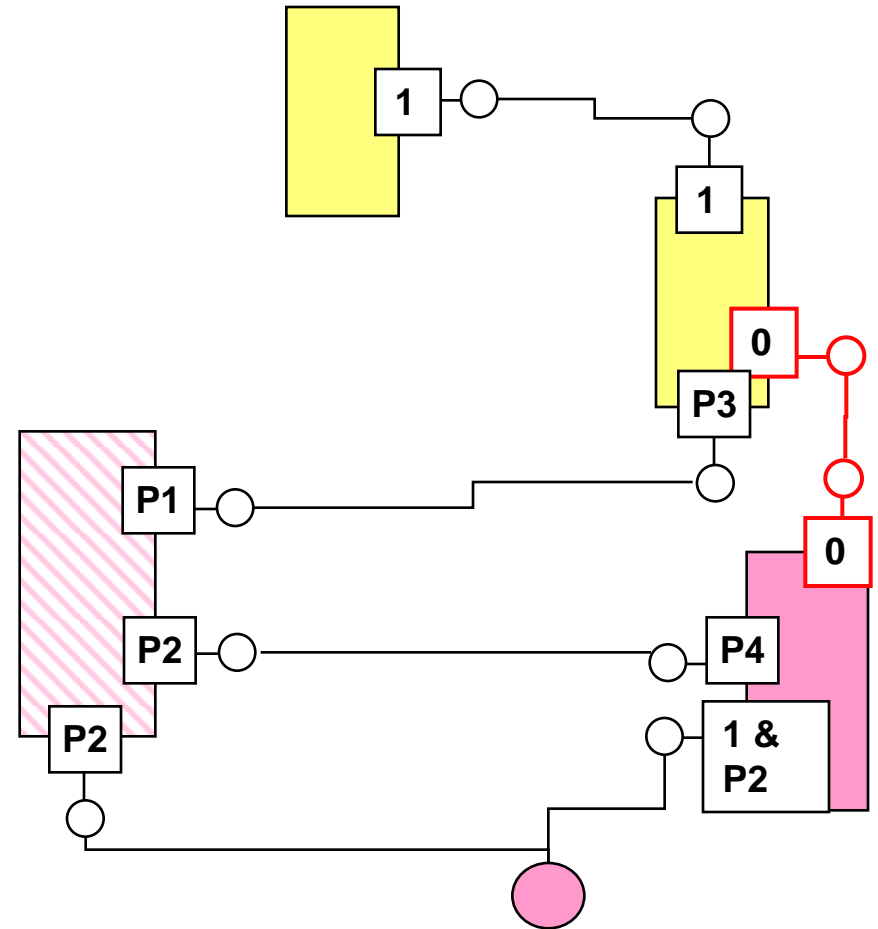
		To TVD:		
From TVD:		1	P1	P2
		P3	1	0
		P4	0	1

## Flow Policy:

- Source/Target: TVD + Machine Type
- Flow: Protocol spec

## Enforcement:

- Absence of virtual connections
- Firewall rules

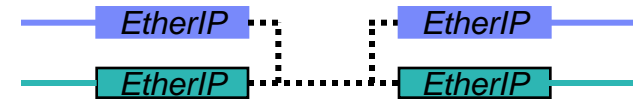


## Isolation and Confidentiality: Virtual Networking Elements

### ▪ EtherIP Encapsulation

- Encapsulate VM Ethernet frames in IP packets
- Allows VLAN over TCPIP/VPN
- RFC3378: EtherIP standard is used for encapsulation

**Security:** Isolation on non-VLAN Integrity-preserving Network



### ▪ VLAN tagging

- A more efficient alternative for EtherIP in data-centers
- Used to tag VM Ethernet frames to denote VLAN membership

**Security:** Isolation on Integrity-preserving VLAN Network



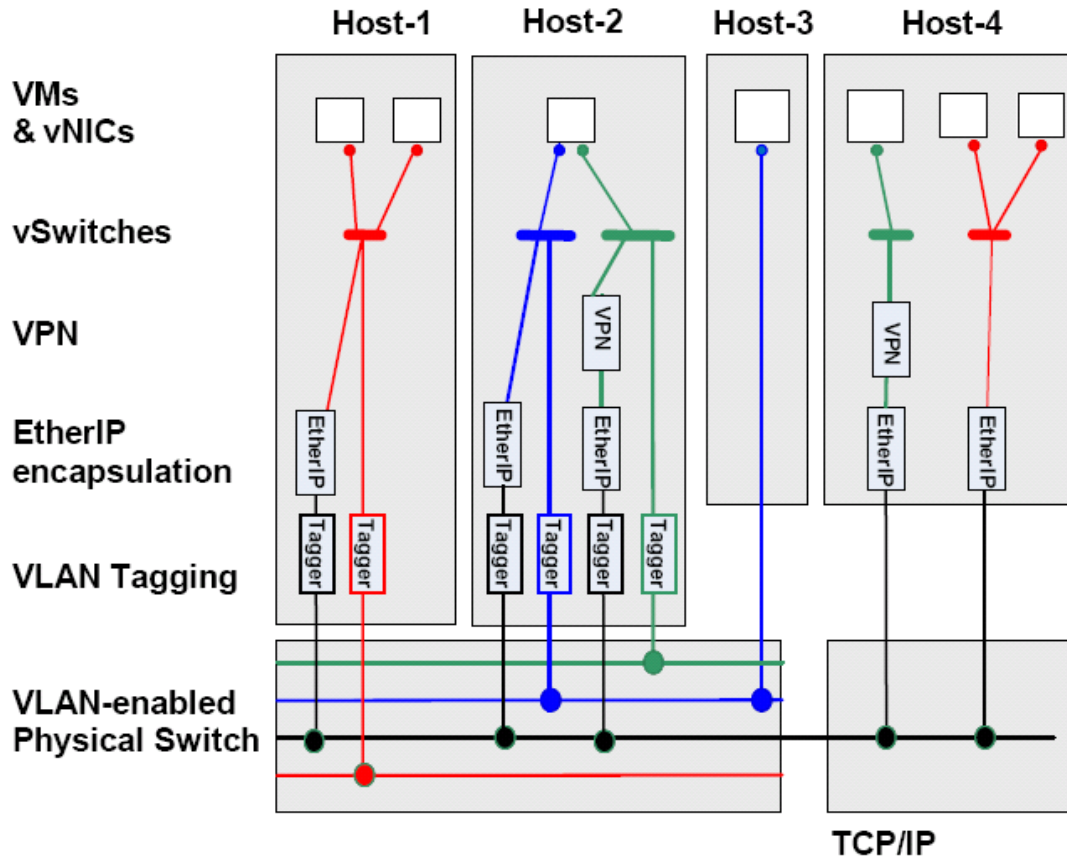
### ▪ Virtual Private Network (VPN)

- Protection of transport on untrusted networks

**Security:** Confidentiality/Integrity of Transport



# Auto-Provisioned Networking Infrastructure



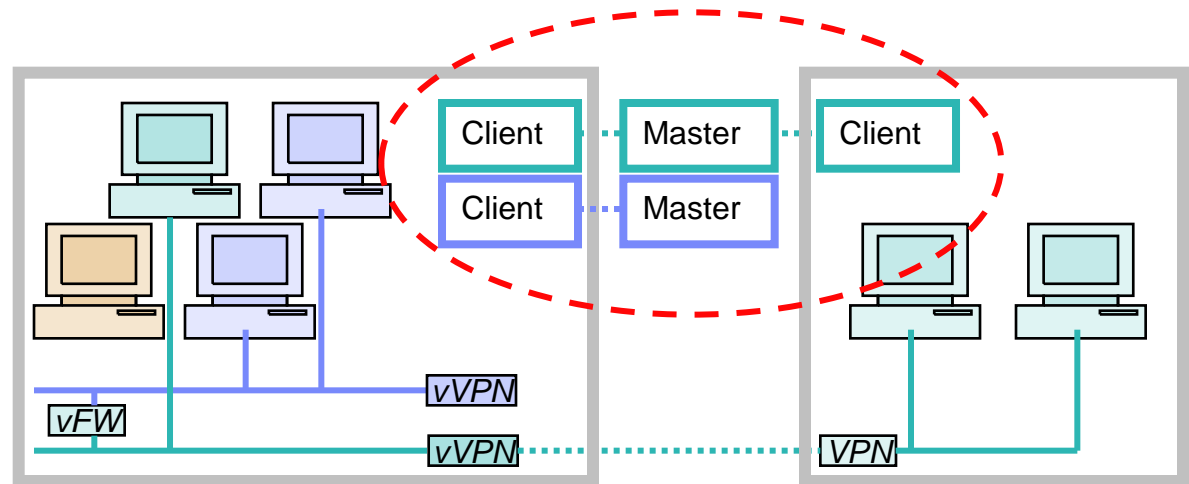
### 3 Management Rules:

- Untrusted physical network
  - Requires VPN
- Non VLAN network
  - Requires EtherIP
- VLAN network
  - Requires Tagging

### Challenges:

- VLAN and EtherIP
- Mix of virtual and physical machines in VLAN
- Admission control
  - VLAN
  - Virtual Machine
  - EtherIP

# Policy Management System



## TVD Master/Client

= Domain Policy Server

- Defines policy
- Key management
- Global admission control
- Global network knowledge

## Usage by End-Users

1. Admin: Declares domain policies
2. User:
  1. "Expand" a domain to local machine
  2. Connect a VM to a domain

# Conclusion

## Lessons Learnt

- Users do not need to care about security
- Generated layout can be audited

## Open Questions

- Right level of abstraction / admin involvement
- Trust management for
  - Infrastructure
  - Gateways
  - Partners

## For more information ...

- How to reach me
  - Matthias Schunter <mts@zurich.ibm.com>
  - <http://www.zurich.ibm.com/~mts>
  - [Phone +41 \(1\) 724-8329](tel:+417248329)
  
- IBM Research
  - IBM Zurich Research Lab: <http://www.zurich.ibm.com>
  - Security research at IBM:  
<http://www.research.ibm.com/compsci/security>
  - IBM Privacy Research Institute:  
<http://www.research.ibm.com/privacy>
  
- OpenTC Project: <http://www.opentc.net>

# Appendix – Extra slides

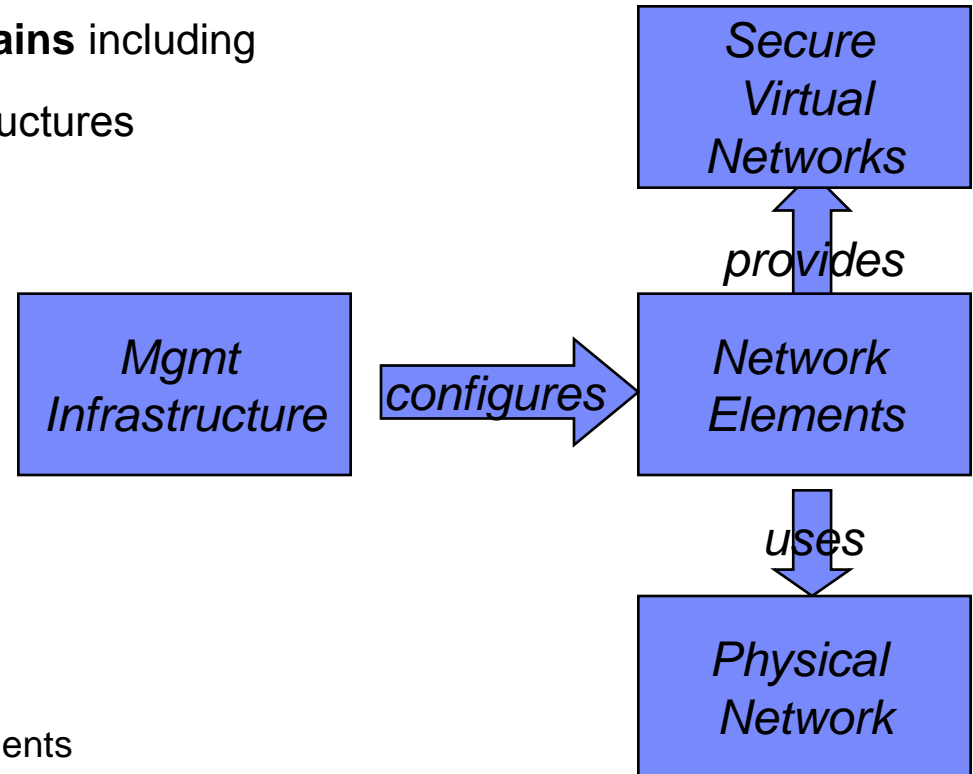
# Building Blocks for Secure Virtual Networks

## Goal: Trusted Virtual Domains

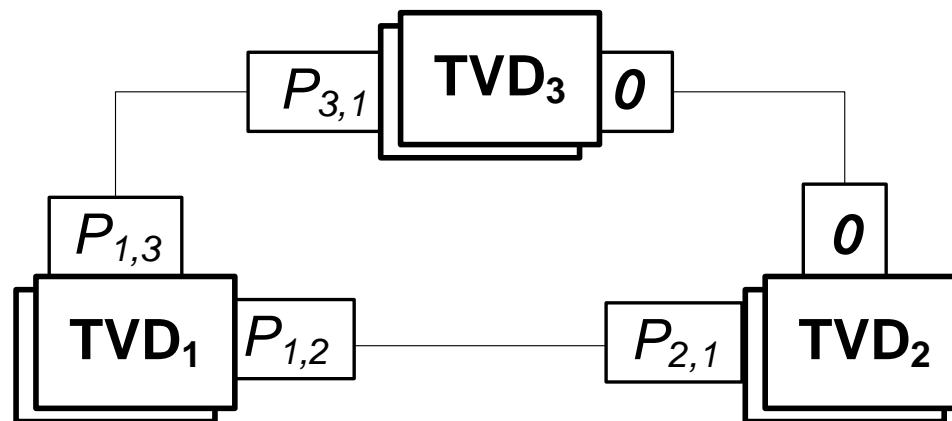
- Cross-machine **Trusted Virtual Domains** including Machines and Networks
- ...for various physical network infrastructures (VLAN, Ethernet, TCP/IP)

## Building Blocks:

- **Physical Network**
  - Trusted/untrusted wrt confidentiality/integrity
  - With/without built-in isolation
- **Network Elements**
  - Allow to provide isolated and protected virtual networks
  - on arbitrary physical network
- **Management Infrastructure**
  - Selects and configures network elements
  - ... to provide desired protection and flow control (security policy)
  - ... on a given physical network (given capabilities)



## Policies and Flow Control for Trusted Virtual Domains

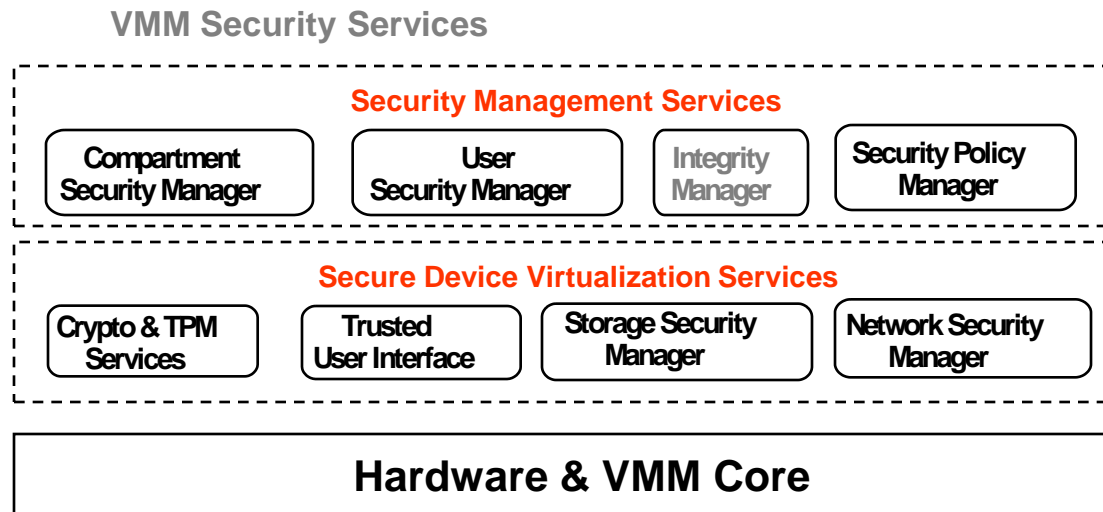


### Security Policies:

- Transport protection (confidentiality, integrity) per TVD
- Flow control:

from/to	$TVD_1$	$TVD_2$	$TVD_3$
$TVD_1$	$1^*$	$0^*$	$P_{13}$
$TVD_2$	$0^*$	$1^*$	$0$
$TVD_3$	$P_{31}$	$P_{32}$	$1$

# High-level Architecture



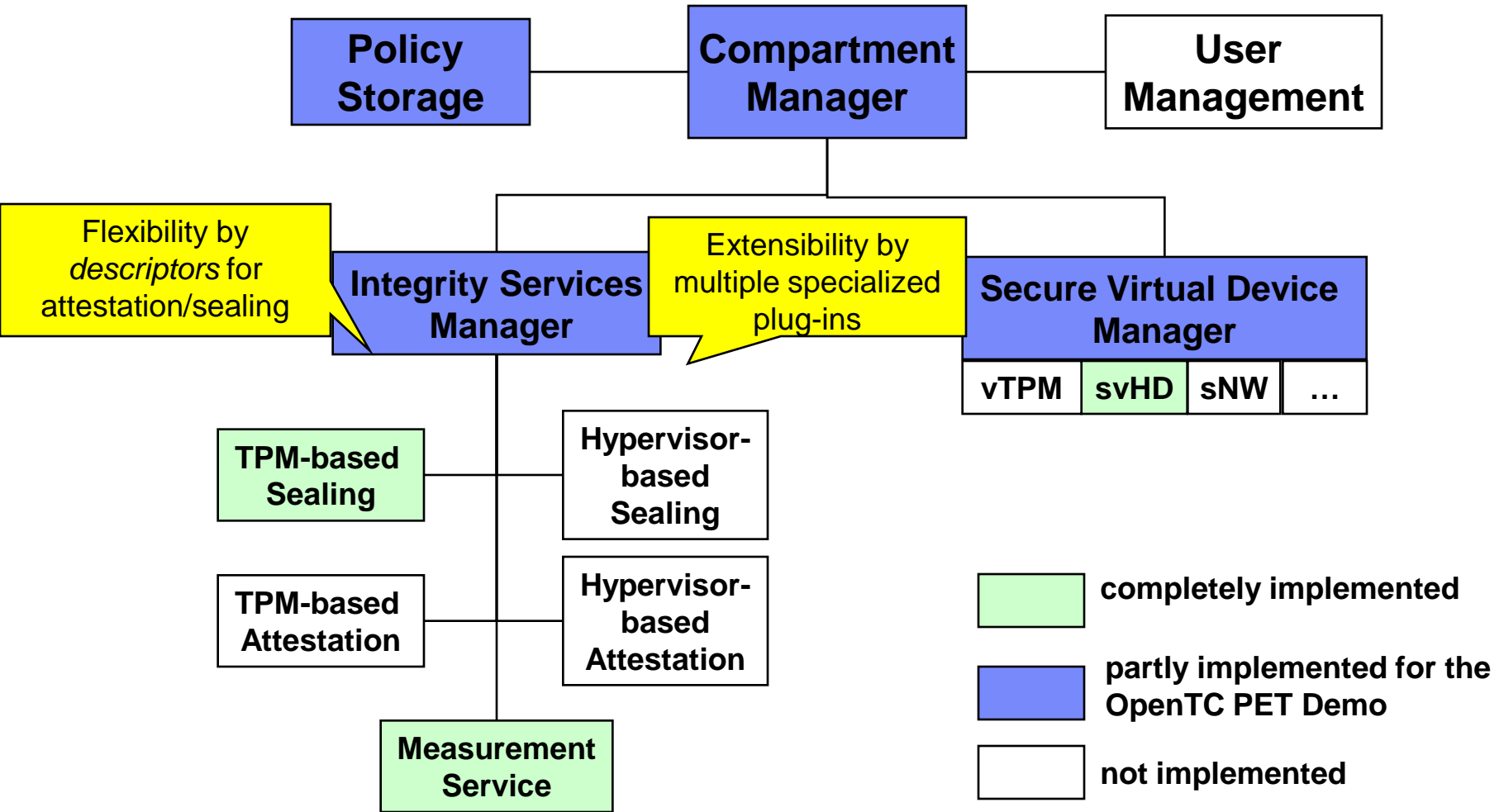
## ■ Device Services

- security-enhanced virtualization of devices
- network, block devices, access control: USB, PCI, vTPM, VNC
- others?

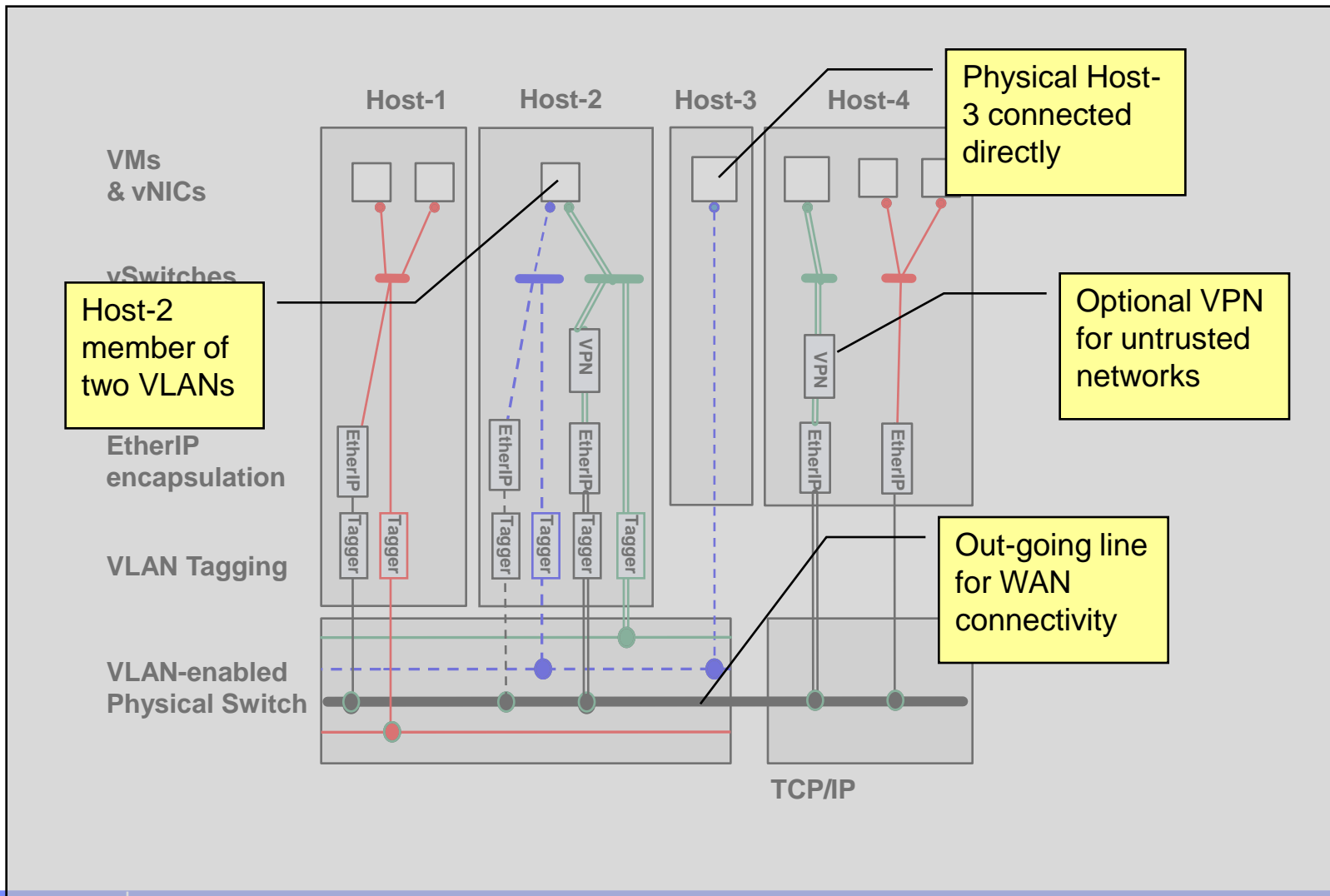
## ■ Management Services

- unified view on maintain a unified view on security guarantees that cover multiple devices and the VMM core

# Current Status of Implementation



# Virtual Networking Composition



# Some Publications

- **Enhancing Grid Security Using Trusted Virtualization.** H. Löhr, H.V. Ramasamy, A-R. Sadeghi, S. Schulz, M. Schunter, C. Stüble. Proceedings of the 4th International Conference on Autonomic and Trusted Computing (ATC-2007), pp. 372-384
- **Architecting Dependable Systems Using Virtualization.** H.V. Ramasamy, and M. Schunter. Workshop on Architecting Dependable Systems: Supplemental Volume of the 2007 International Conference on Dependable Systems and Networks (DSN-2007), To appear.
- **Towards Automated Provisioning of Secure Virtualized Networks.** S. Cabuk, C. Dalton, H.V. Ramasamy, and M. Schunter. Proceedings of the ACM Conference on Computer and Communication Security (CCS 2007), To appear.
- **Enabling Fairer Digital Rights Management with Trusted Computing.** A-R. Sadeghi, M. Wolf, C. Stueble, N. Asokan, and J-E. Ekberg. Proceedings of the Information Security Conference 2007 (ISC-2007), To appear.
- **Phishing phishers - observing and tracing organized cybercrime.** D. Birk, S. Gajek, F. Grobert, and A-R. Sadeghi. In IEEE Cyberfraud, 2007, To appear.
- **Compartmented Security for Browsers - Or How to Thwart a Phisher with Trusted Computing.** S. Gajek, A-R. Sadeghi, C. Stueble, and M. Winandy. Proceedings of the Second International Conference on Availability, Reliability and Security (ARES 2007), To appear.
- **Beyond Secure Channels.** N. Asokan, Y. Gasmi, A-R. Sadeghi, P. Stewin, M. Unger. Proceedings of the ACM Workshop for Scalable Trusted Computing 2007, To appear.
- **Reconfigurable Trusted Computing in Hardware.** T. Eisenbarth, T. Güneysu, C. Paar, A-R. Sadeghi, D. Schellekens, and M. Wolf. Proceedings of the ACM Workshop for Scalable Trusted Computing 2007 (short paper), To appear.
- **Realizing Property-Based Attestation and Sealing with Commonly Available Hard- and Software.** U. Kühn, M. Selhorst, and C. Stüble. Proceedings of the ACM Workshop for Scalable Trusted Computing 2007, To appear.

# Physical Infrastructures

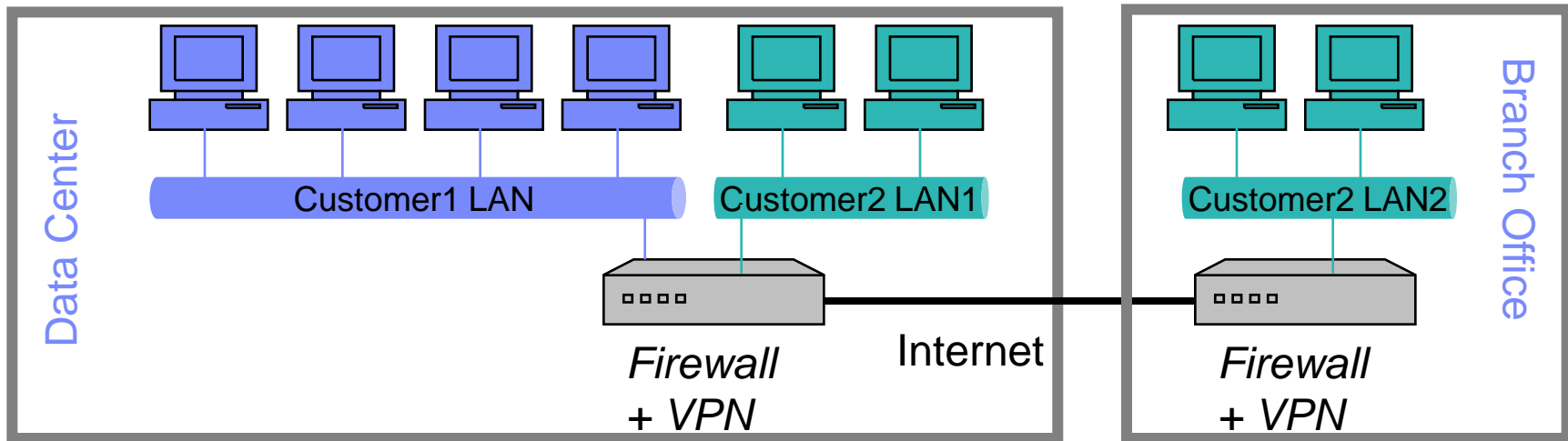
## Transport

- VLAN-enabled Physical Switch
  - Connects two or more VLAN segments belonging to the same or different VLANs
  - Each VLAN segment is connected to a port on the VLAN switch
  - Guarantees isolation among different VLAN segments
- Non-VLAN Switch (Ethernet network)
- TCP/IP Network / Internet

## Trusted/Untrusted Networks:

- Confidentiality / integrity (e.g., inside datacenter)

# Today's Data Centers



## Today's Data Center Infrastructure:

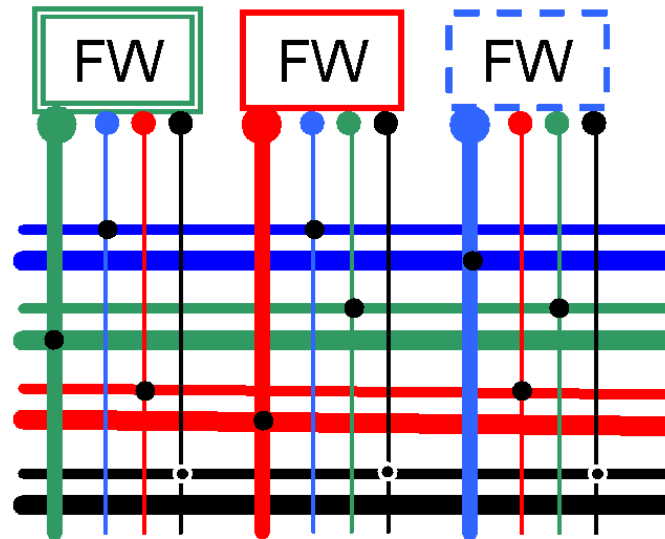
- Networking: VLAN, Internet, VPN
- Machines: Racks of servers

## Today's Security:

- Customer isolation – One “cage” per customer
- Flow control - Firewalls
- Transport protection – VPN Routers
- Network admission control – cables are plugged in or not

## How can a virtual datacenter be secured?

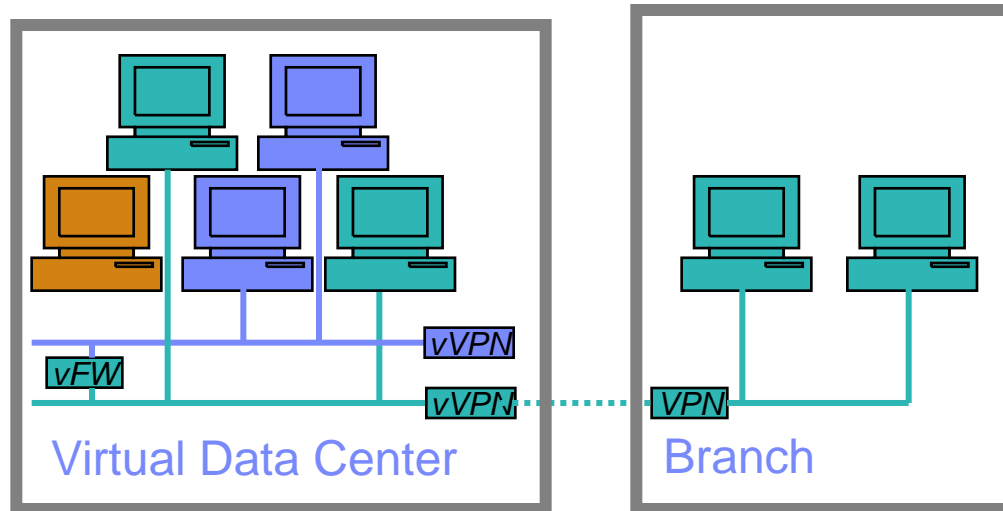
# Interconnects and Flow Control



## Core Ideas:

- 2 Networks per color: Internal and interconnect
- Absent interconnect (No “•”) enforces  $0$  policy
- Firewall rules enforce  $P$  policies

# Goal: Secure Virtual Datacenter



## Secure Cross Machine Virtual Security Zones (Trusted Virtual Domains)

- Machines, Networks, Network devices (FW, VPN)
- Transparent to end-users

## Security of TVD must not rely on untrusted components:

- Confidentiality/Integrity (transport security)
- Network admission control
- Flow control