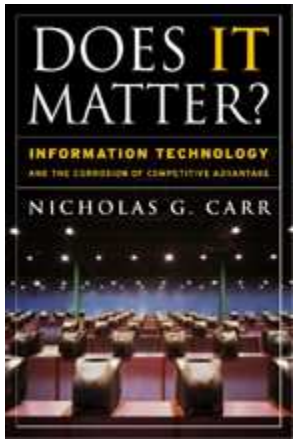
CERT - NETWORKS… what networks?

Mohamed Ibrahim,
Research Fellow, Melbourne University
Senior Advisor – MIPT, Somalia
.so ccTLD Manager



CERT - NETWORKS… what networks?

Theme:

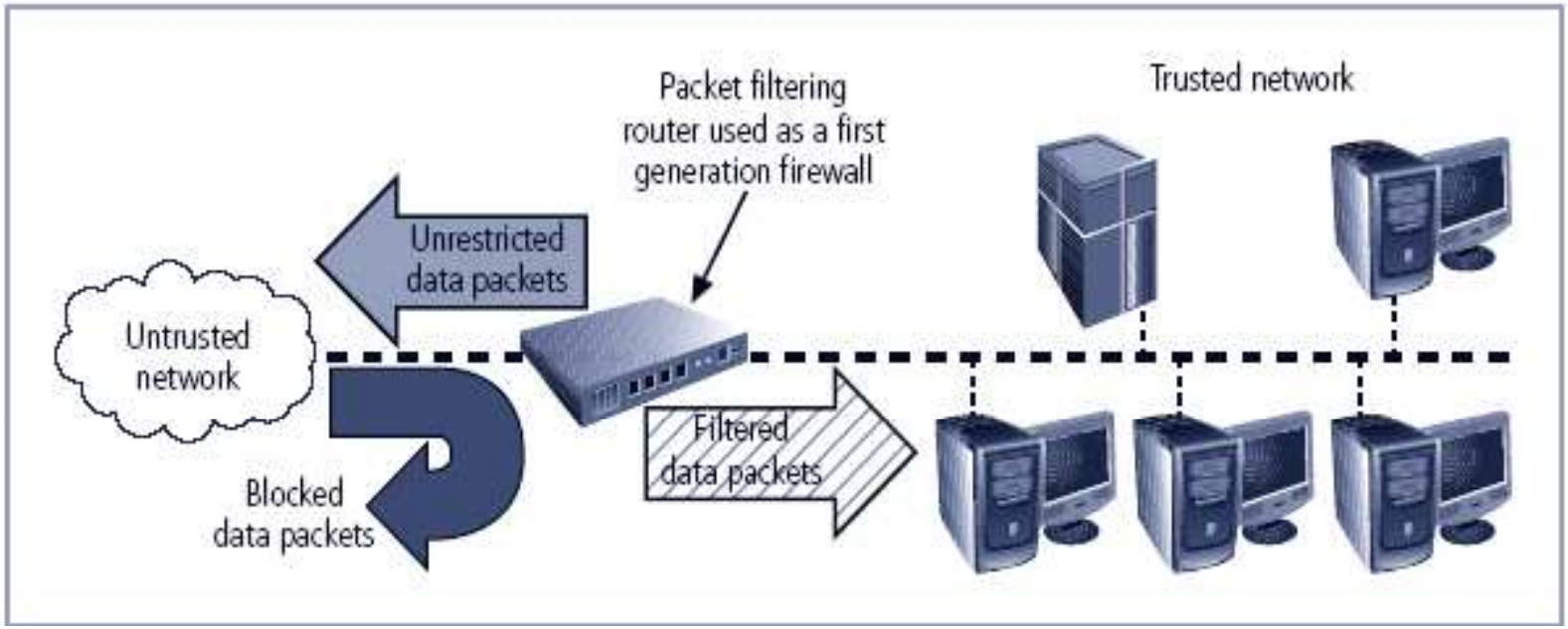
- Global Concern
- Global Response
- African Response
- National Respnse
- CSIRT

Learning Objectives

Upon completion of this material, you should be able to:

- Understand Networks and Related security issues
- Describe the technology that enables the
- security environment of Networks
- Trusted Networks
- Cloud computing

CERT - NETWORKS… what networks?



Trusted Networks… Really?

Global Concern:
A World Under Attack

Web War I

Estonia: World's most wired nation
April 27, 2007: CyberAttack
Denial of Service Attack
Attack came from various servers from South America, Europe, Asia
Swamped the websites of Estonia's private and public organizations

CERT? CSIRT?

- CERT = Computer Emergency Response Team
- CSIRT = Computer Security Incident Response Team

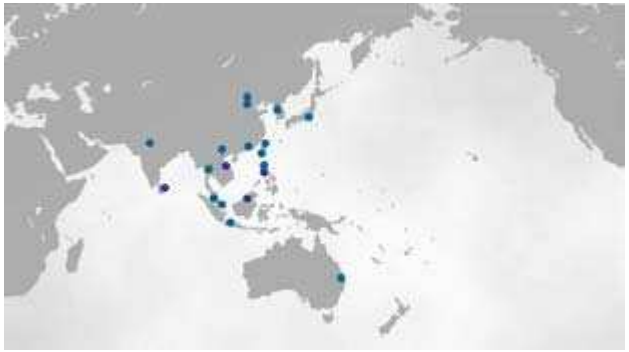
The Geeky Side

- Artifact analysis
- Malware analysis
- Vulnerability analysis
- Network monitoring
- Technology research

CERT - is there anyone out there?

Asia Pacific CERT
Economies Covered

Australia
Bangladesh
Brunei
China (PROC)
Chinese Taipei
Hong Kong
India
Indonesia
Japan
Korea
Malaysia
Philippines
Singapore
Sri Lanka
Thailand
Vietnam



CERT - Examples from Home ….

SOCERT

A member of AFCERT

- Point of Contact
- Coordination with other CERTs/CSIRTs
- Incident handling and Management
- Information dissemination
- Pass on Alerts, warnings, and advisories
- Awareness and Education
- Policy Development
- Legislative support
- Rules and regulation development
- Coordination with Law Enforcement

CERT - NETWORKS… what networks?

Challenges:

- Resolve incidents at the shortest time possible
- relevant/avoid the occurrence of such incidents
- Mitigate impact and minimize damage

CERT - NETWORKS… what networks?

Information Security Practice in Somalia

- Certified information security professionals
- Organizations maintain information system security teams

CERT - NETWORKS… what networks?

Why Create CERTs/CSIRTs

- Best practice
- Obligation to stakeholders
- Protection of the organization
- Information Gathering
- ncident coordination

CERT - NETWORKS… what networks?

Why Create CERTs/CSIRTs

- Quickly respond to security incidents
- Quickly resolve security breaches
- Promote information security awareness, discipline, and practice
- Preparedness and adopting an information security culture are keys to protecting our most valuable information assets.

CERT - NETWORKS… what networks?

Incident Handling and Management
Process and Practice

- Prepare
- Gather information
- Vulnerability Information
- Security Reports, Bulletins, and Alerts
- Reports on malicious activities
- Malware information

Incident Handling and Management
Process and Practice
- Protect
- Firewalls
 -Intrusion Prevention Systems
 -Intrusion Detection Systems
 -Harden systems and applications
- Update and apply patches

Incident Handling and Management Process and Practice:

Monitoring =>Detection=>Response=>Resolution

3C Framework : Cooperate => Collaborate => Coordinate

Document

Gather information:
Vulnerability Information =>Security Reports, Bulletins, and Alerts
Reports on malicious activities =>Malware information
Keep watch

Request and exchange information with other CERTs/CSIRTs
if host is in other jurisdiction, request CERT/CSIRT in that jurisdiction for assistance

Incident Handling and Management Process and Practice:

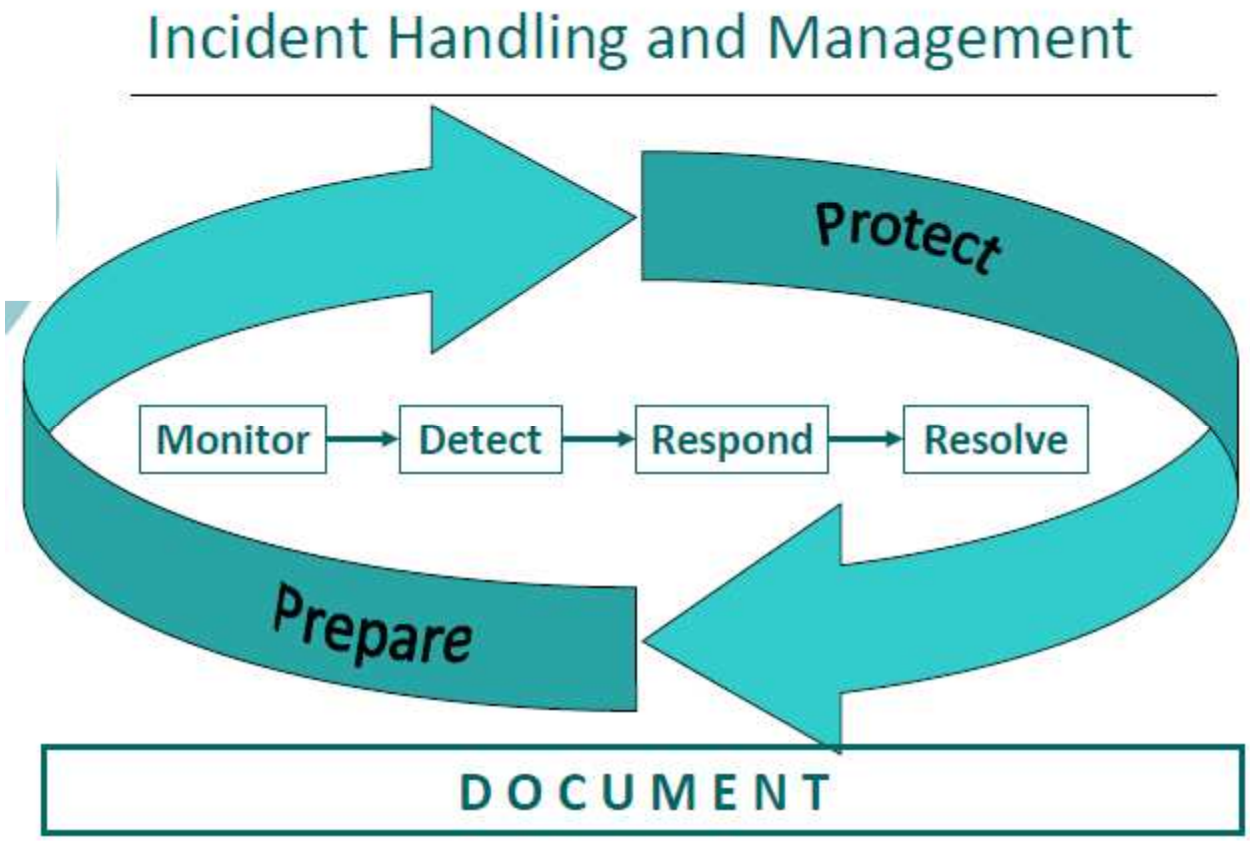
- Network Monitor
- Anomalous activities
- Unusual traffic
- Intrusion detection system
- Incident report

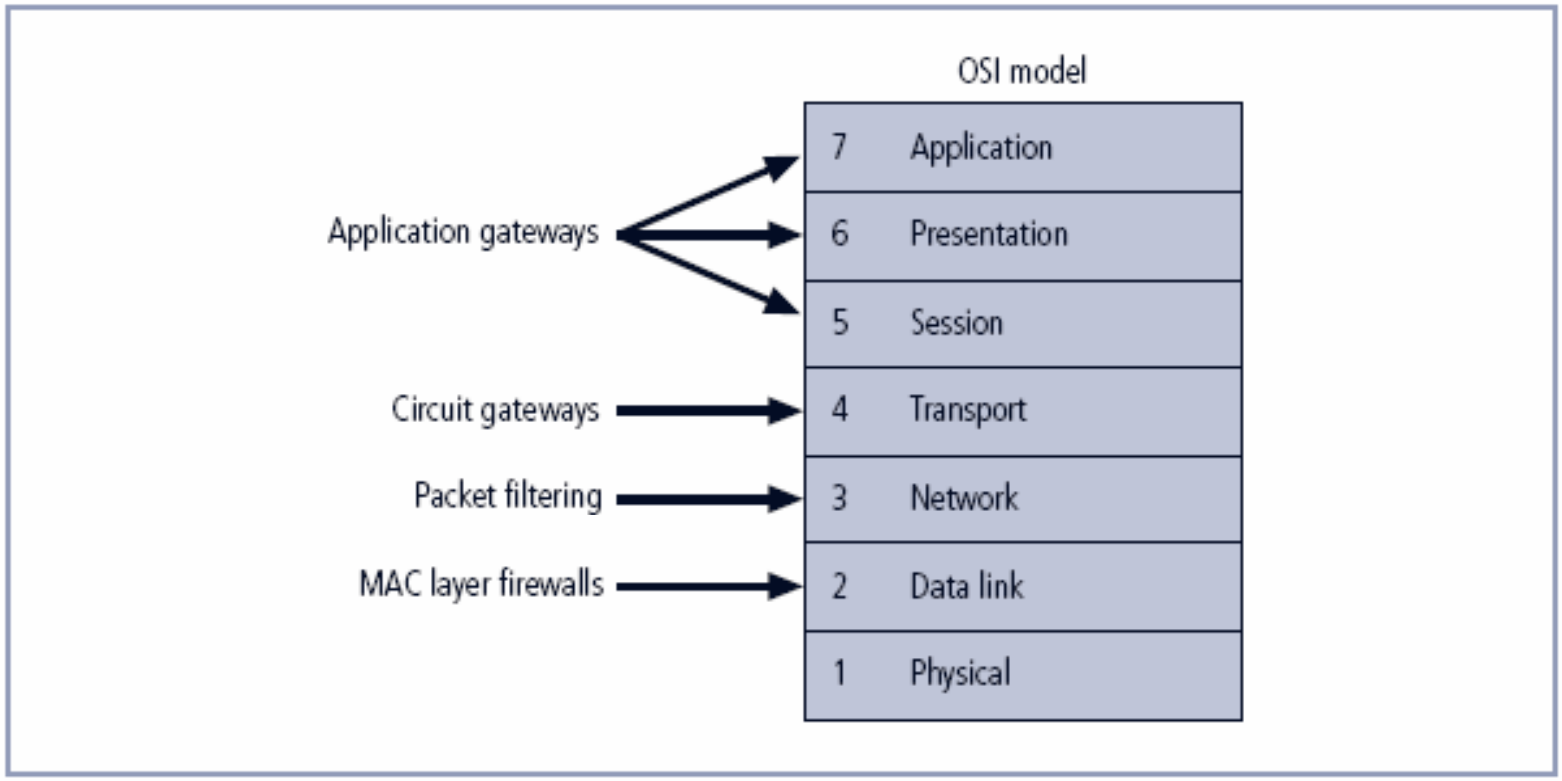
- Triage
- Identify
- Categorize
- Prioritize
- Escalate

- Known incident: execute appropriate response
- Unknown; Escalate to Malware Analysis
- Capture => Analyze => Develop response => Resolve

Incident Handling and Management Document:

- Incident ticketing system
- Monitor / track incidents until resolution
- Keep / hold in database
- Incident type, description, class, priority
- Keep record of analysis
- Templates
- Acknowledging reports
- Request for information
- Bulletins, Alerts


Incident Handling and Management
Protect
Monitor
Detect
Respond
Resolve
Prepare
DOCUMENT



The Open Systems Interconnection model (**OSI model**)

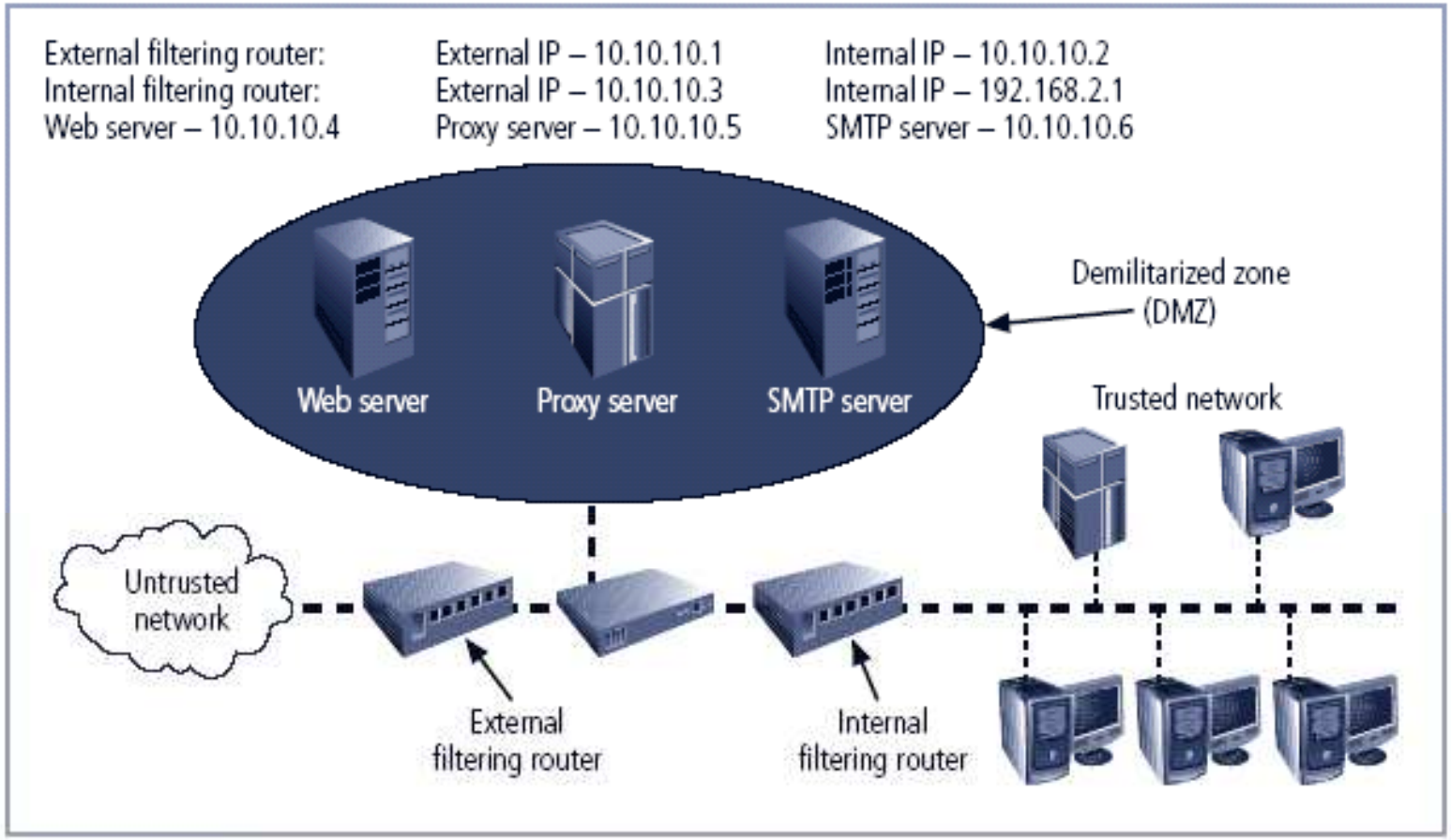
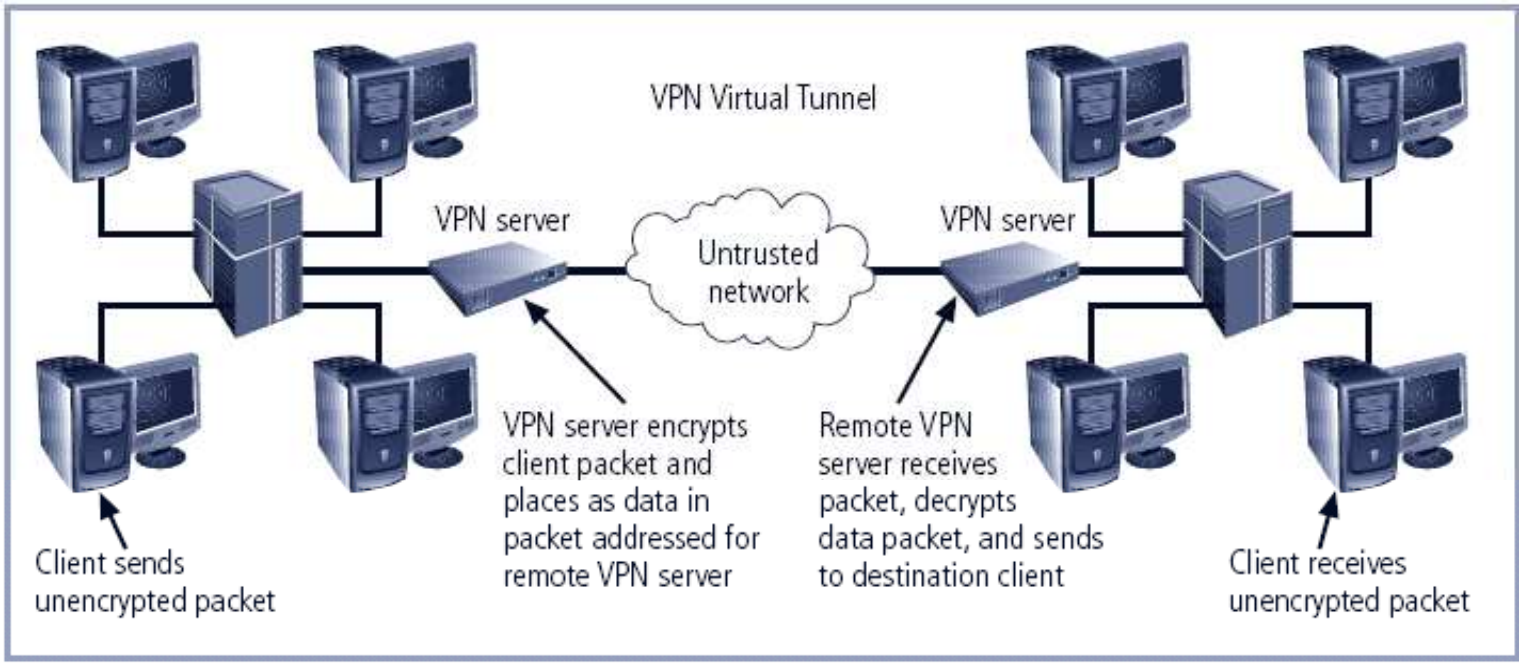
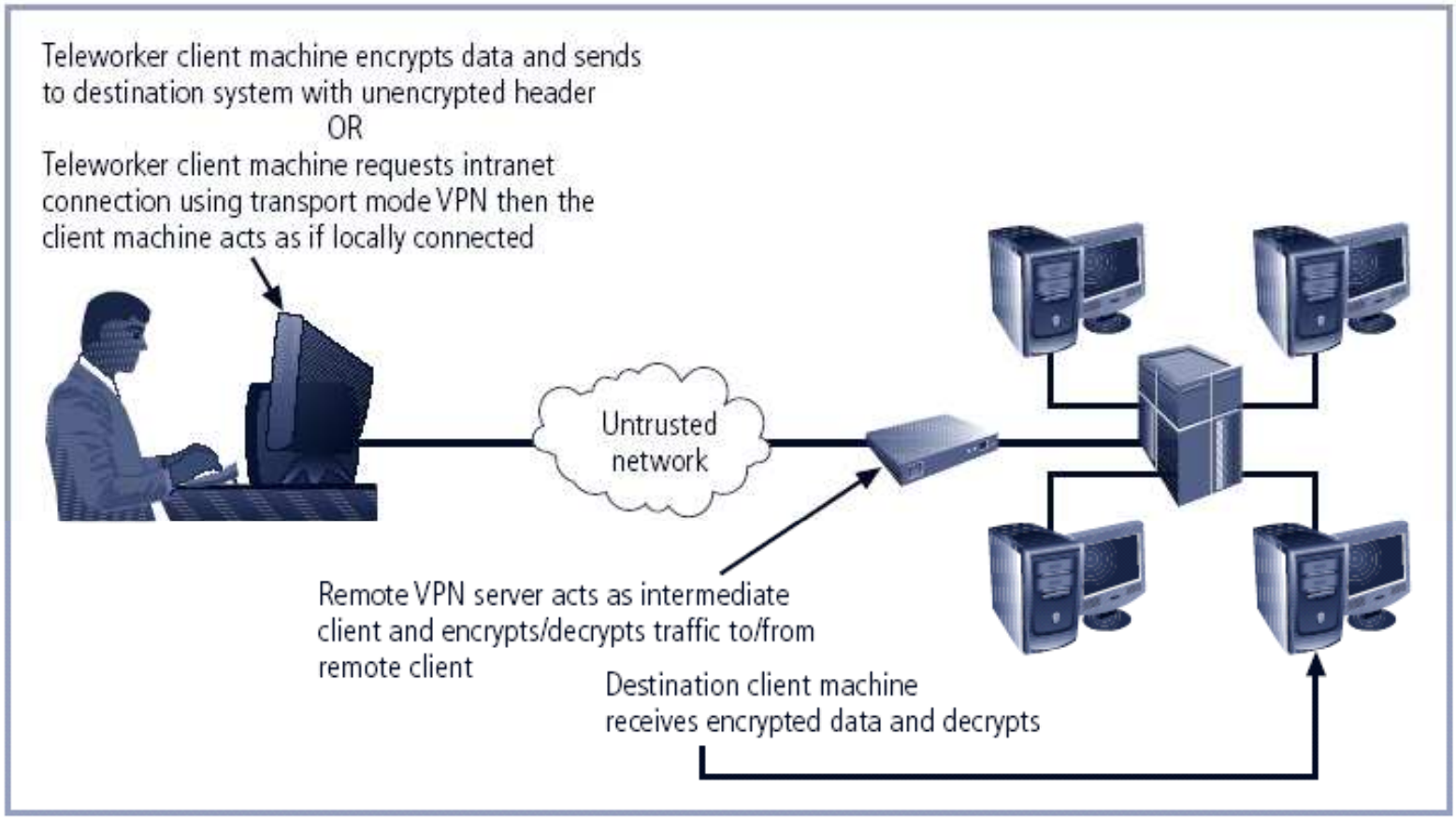


FIGURE 6-14 Example Network Configuration


VPN Virtual Tunnel
VPN server
Untrusted network
VPN server
Client sends unencrypted packet
VPN server encrypts client packet and places as data in packet addressed for remote VPN server
Remote VPN server receives packet, decrypts data packet, and sends to destination client
Client receives unencrypted packet

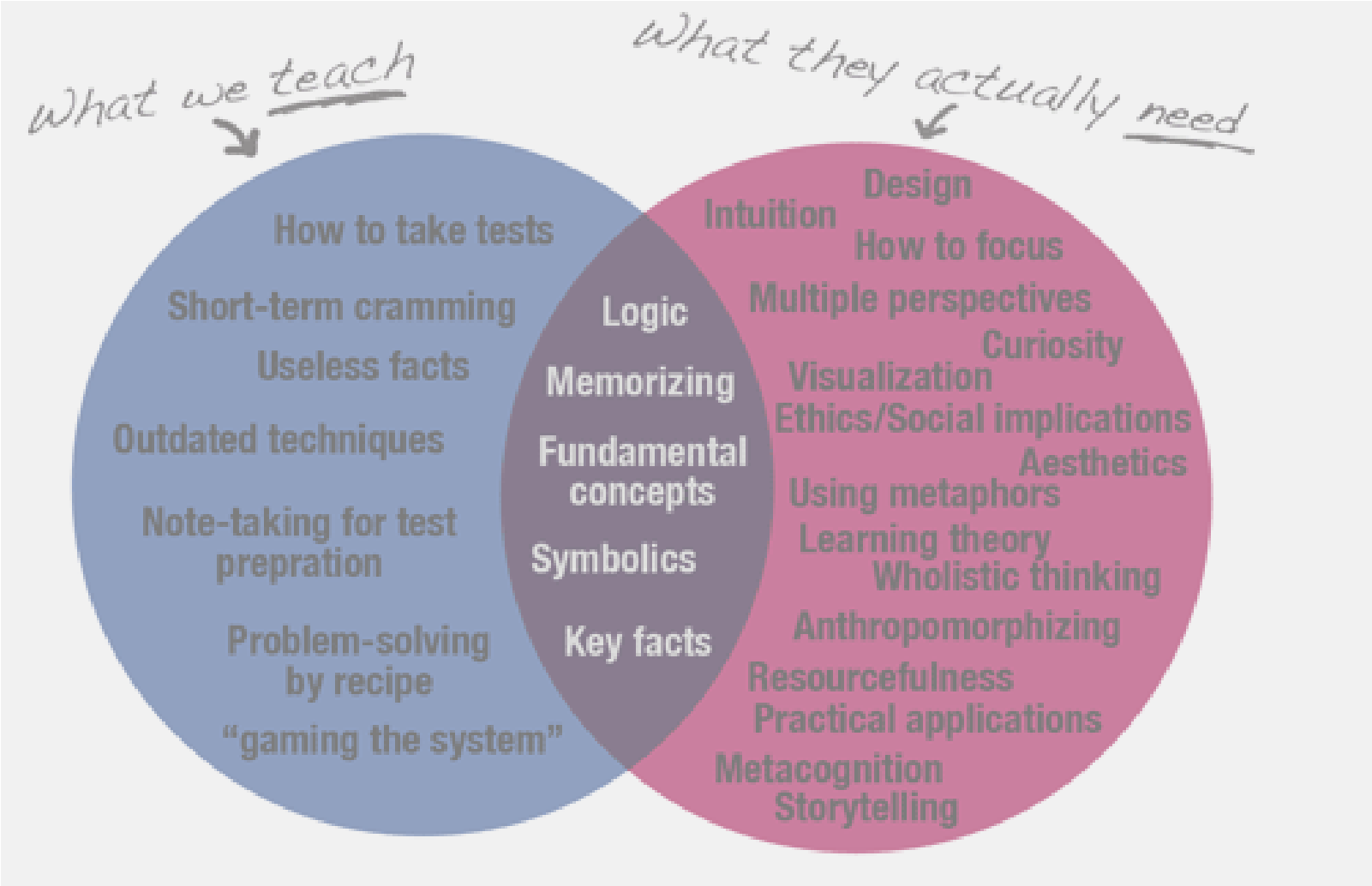

Teleworker client machine encrypts data and sends to destination system with unencrypted header
OR
Teleworker client machine requests intranet connection using transport mode VPN then the client machine acts as if locally connected
Untrusted network
Remote VPN server acts as intermediate client and encrypts/decrypts traffic to/from remote client
Destination client machine receives encrypted data and decrypts

Virtual Private Networks (VPNs)

VPN must accomplish:

- Encapsulation of incoming and outgoing data
- Encryption of incoming and outgoing data
- Authentication of remote computer and (perhaps) remote user as well

Problem? …what problem?



http://headrush.typepad.com/creating_passionate_users/2006/11/why_does_engine.html

Comments welcome

questions…..maybe.