www.CareerCert.info

© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc. for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

www.CareerCert.info

Understanding the Cisco Self-Defending Network

Evaluating Security Solutions for the Network

© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc. for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

www.CareerCert.info

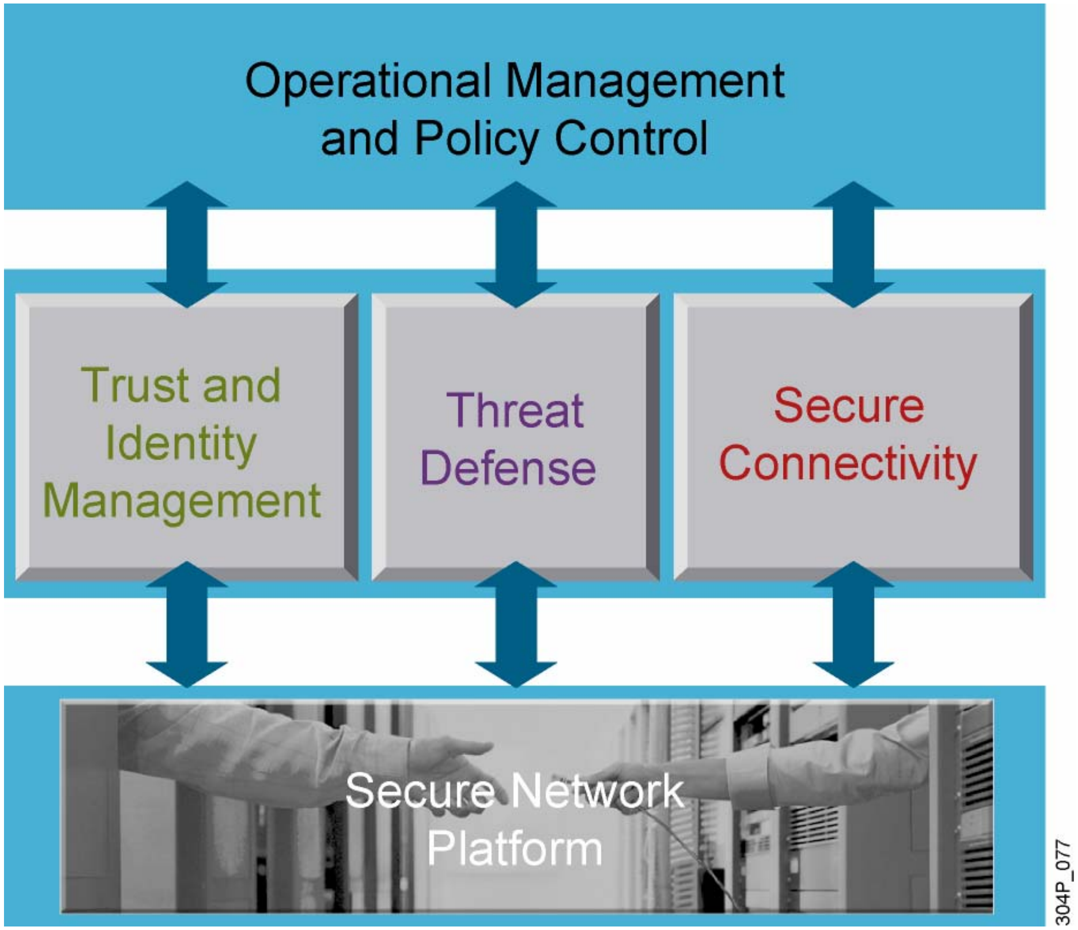
Cisco Self-Defending Network

Efficient security management, control, and response

Advanced technologies and security services to:

- Protect critical assets
- Mitigate the effects of outbreaks
- Ensure privacy

Network as Platform


Operational Management and Policy Control
Trust and Identity Management
Threat Defense
Secure Connectivity
Secure Network Platform
304P_077

© 2007 Cisco Systems, Inc. All rights reserved.

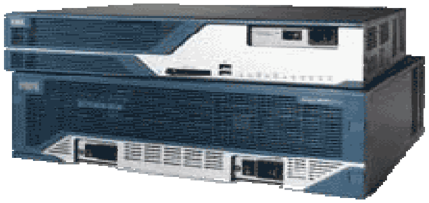
Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

www.CareerCert.info

Network as Platform for Security

- Cisco Integrated Services Routers
  - Integrate Cisco IOS Firewall, VPN, and intrusion prevention system (IPS) services across the Cisco router portfolio
  - Deploy new security features on existing routers using Cisco IOS Software
  - Cisco NAC-enabled
- Cisco Catalyst Switches
  - Denial-of-service (DoS) attack mitigation
  - Integrated security service modules for high-performance threat protection and secure connectivity
  - Man-in-the-middle attack mitigation
- Cisco Adaptive Security Appliances
  - High-performance firewall, IPS, network antivirus, and IPsec/SSL VPN technologies all in one unified architecture
  - Device consolidation to reduce overall deployment and operations costs and complexities
  - Cisco NAC-enabled

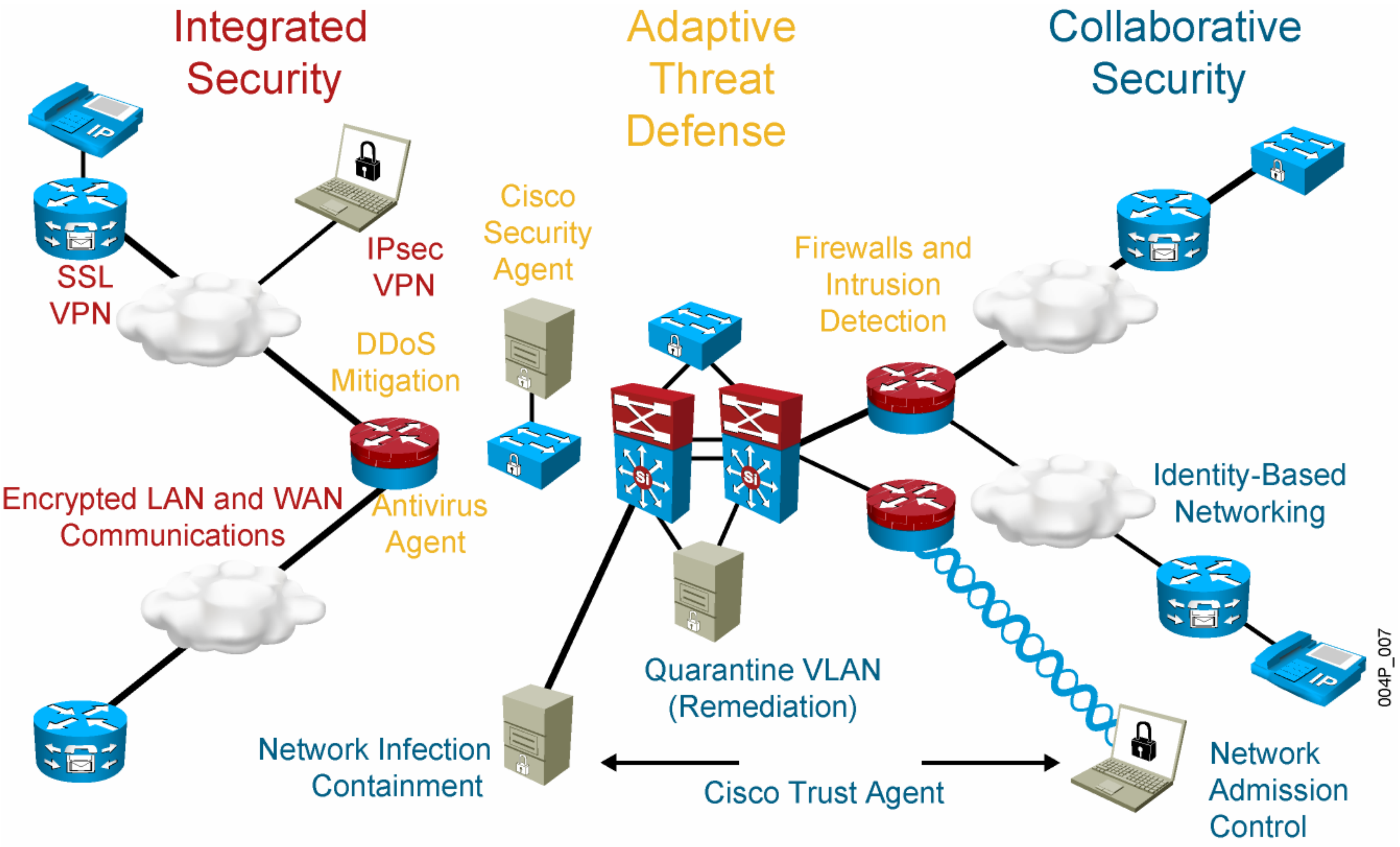


© 2007 Cisco Systems, Inc. All rights reserved.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

Self-Defending Network Phases


Integrated Security
Adaptive Threat Defense
Collaborative Security
SSL VPN
IPsec VPN
Cisco Security Agent
Firewalls and Intrusion Detection
DDoS Mitigation
Encrypted LAN and WAN Communications
Antivirus Agent
Identity-Based Networking
Quarantine VLAN (Remediation)
Network Infection Containment
Cisco Trust Agent
Network Admission Control
IP
Si
004P_007

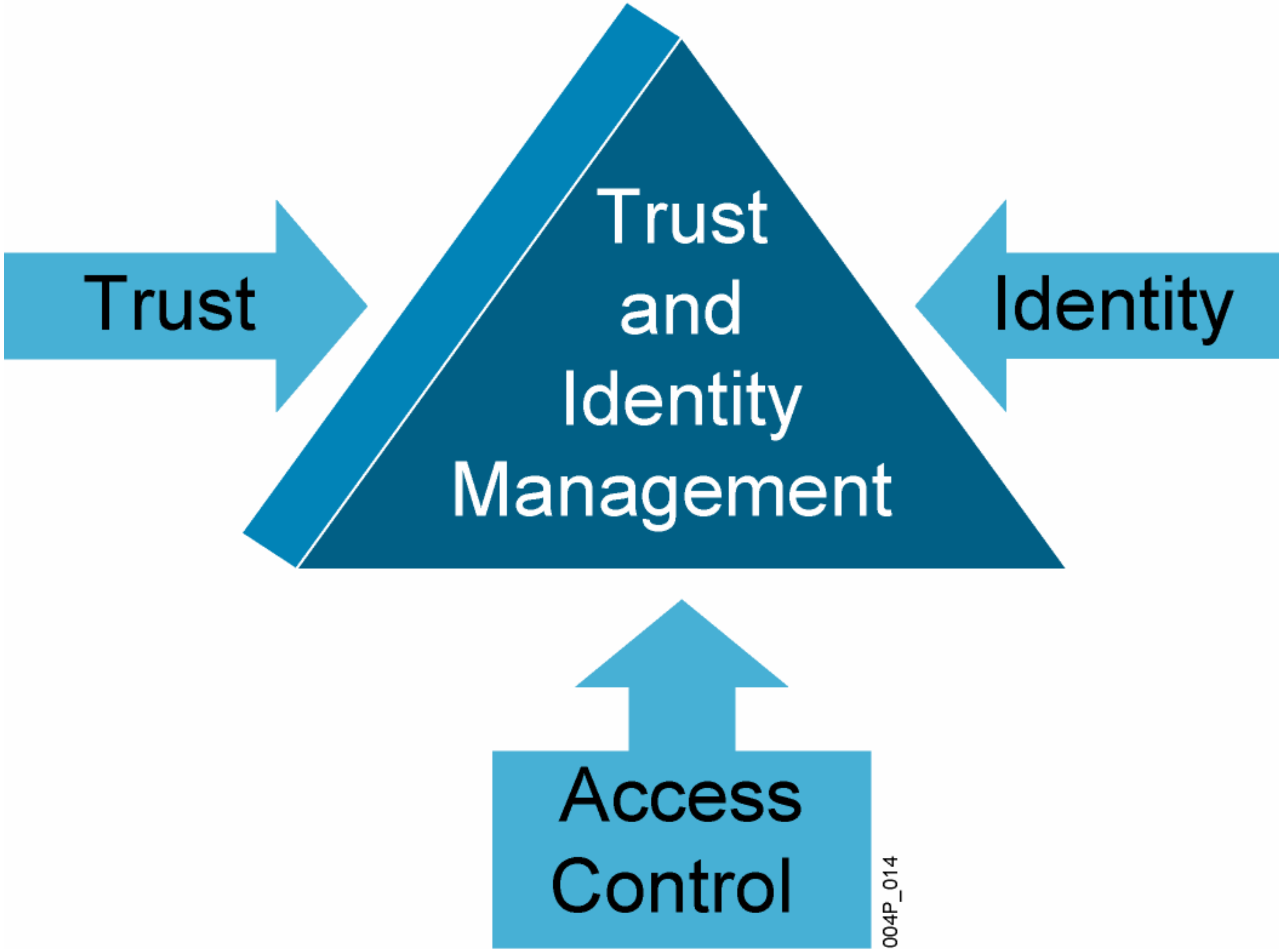
© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

www.CareerCert.info

Trust and Identity Management



© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

www.CareerCert.info

Trust Is the Root of Security

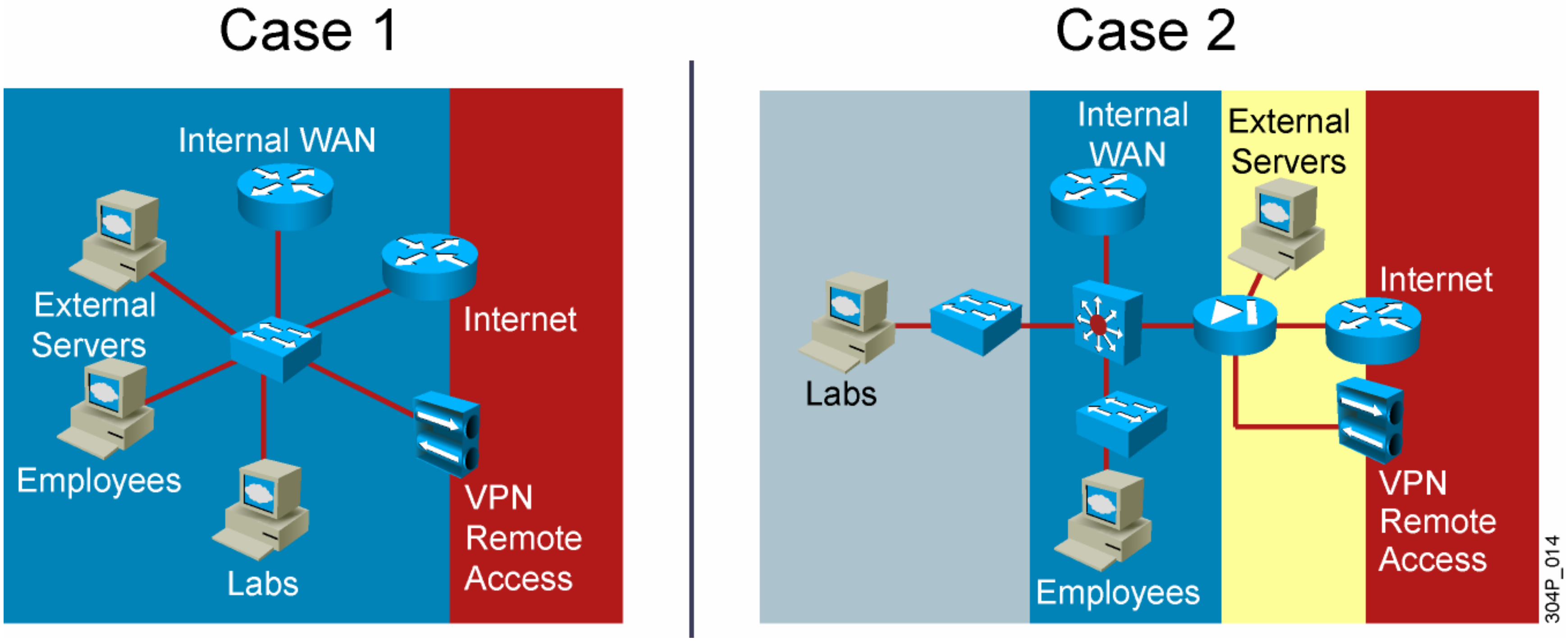
- Trust is a relationship in which two (or more) network entities are allowed to communicate.
- Trust forms the root of all security policy decisions.
- Trust and risk are opposites; security is based on enforcing limitations to trust relationships.
- Trust relationships:
  - Can be explicit or implied
  - Can be inherited
  - Can be abused

© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc. for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

Domains of Trust



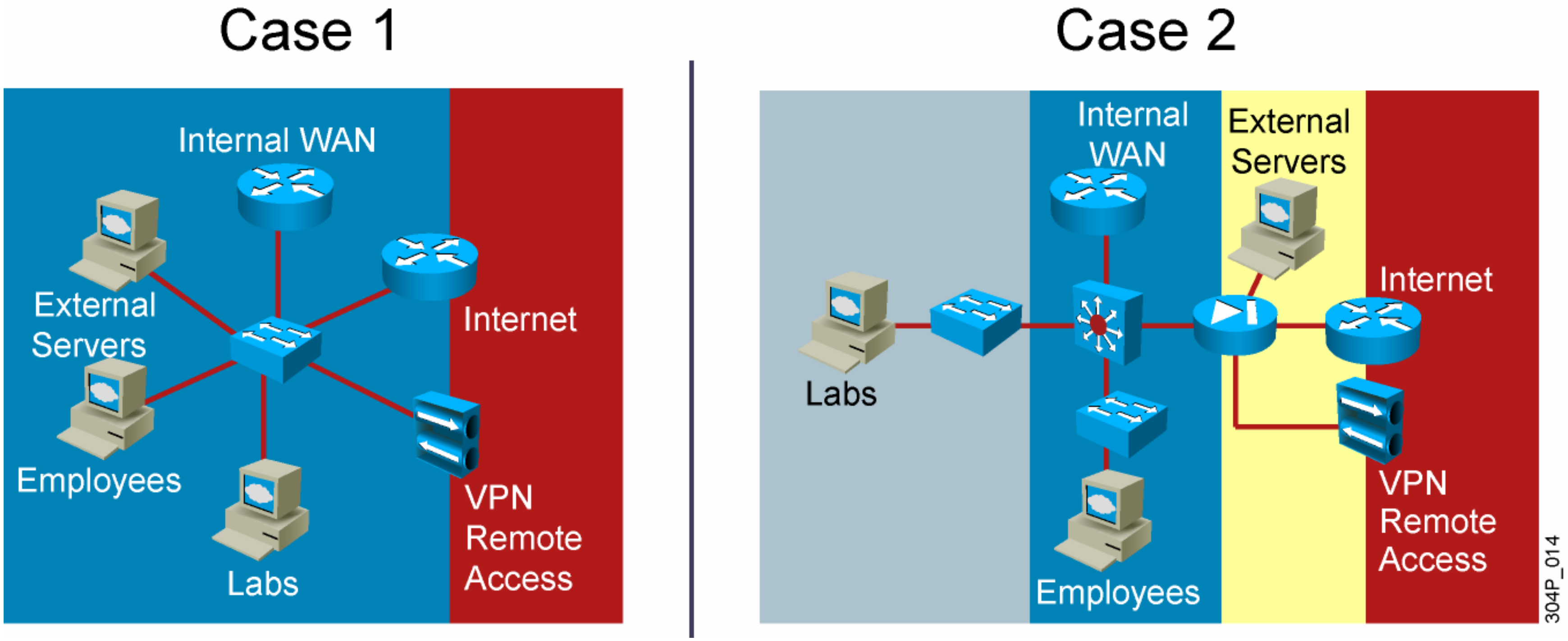
Question: From a security design perspective, what is the key difference between Case 1 and Case 2?

© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc. for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

Domains of Trust



Question: From a security design perspective, what is the key difference between Case 1 and Case 2?

Answer: Case 2 is more segmented into domains of trust.

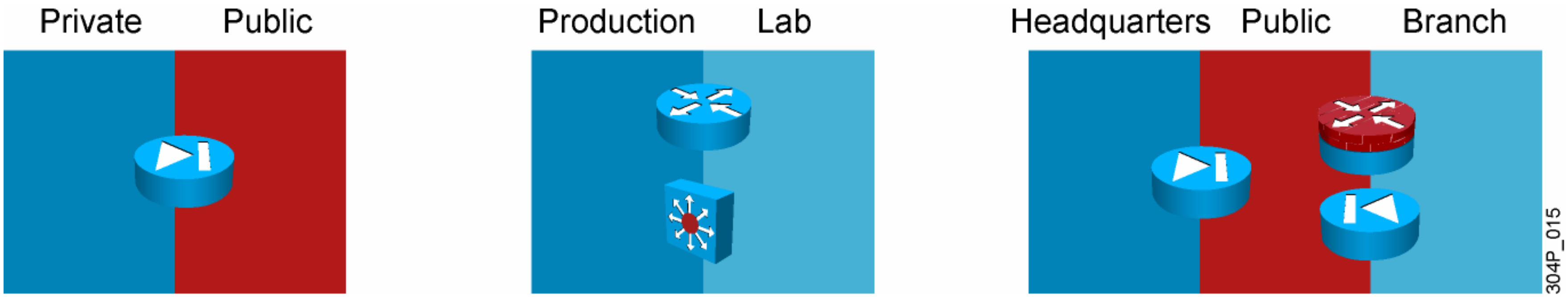
© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

www.CareerCert.info

Example: Domains of Trust



Domains	Gradient	Safeguards Needed
Private to Public	Extreme (high risk)	Advanced firewalling, flow-based inspection, misuse detection (IPS), constant monitoring
Production to Lab	Minor (low risk)	Basic access control, casual monitoring
Headquarters to Branch	Steep (considerable risk)	Communication security, authentication, confidentiality, integrity concerns

© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc. for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

www.CareerCert.info

Identity

Identity is the “who” of a trust relationship. The identity of a network entity is verified by credentials.

- Both people and devices can be authenticated.
- Three authentication attributes:
  - Something you know
  - Something you have
  - Something you are
- Common approaches to identity:
  - Passwords
  - Tokens
  - Certificates

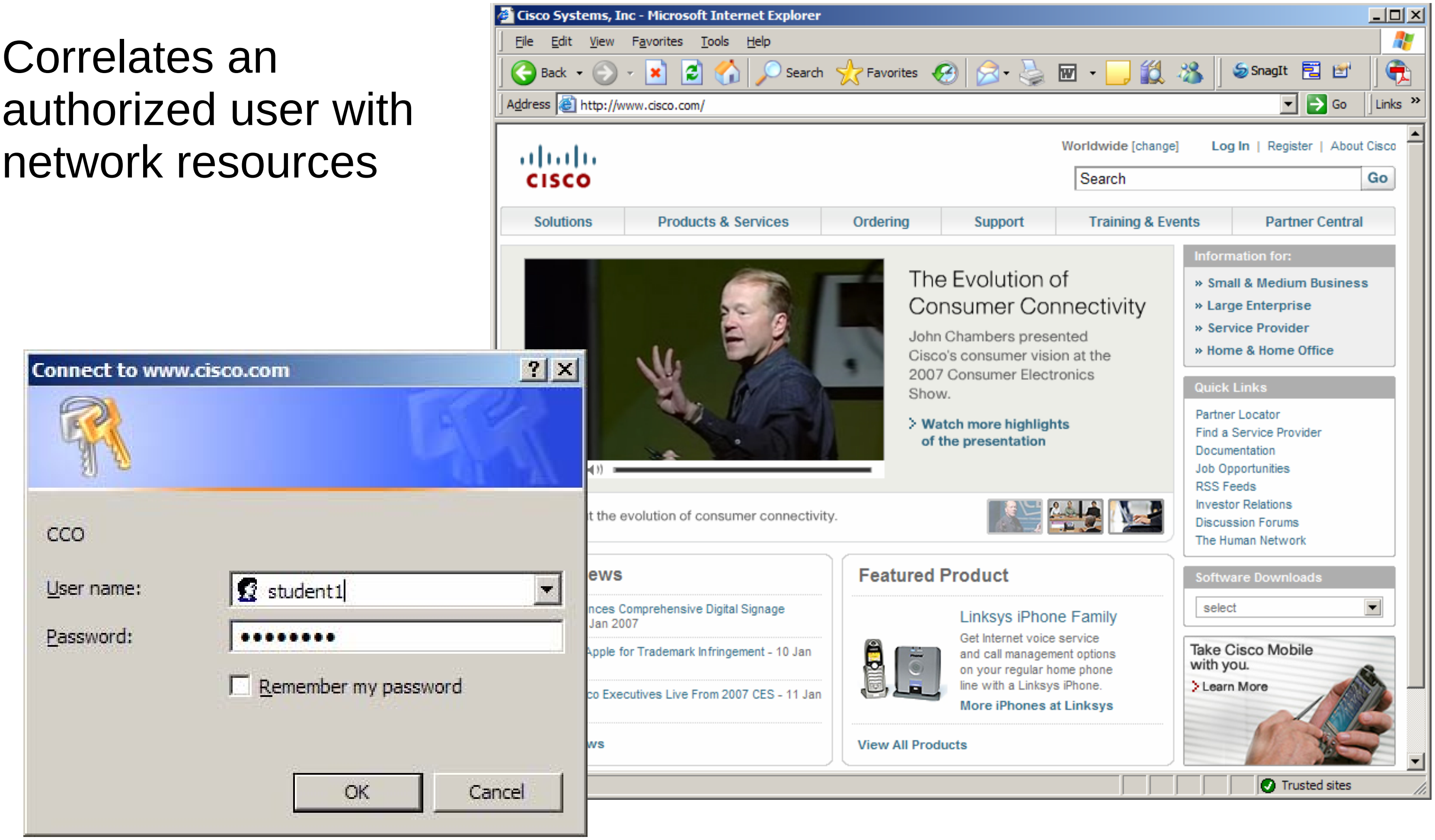
© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc. for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

Passwords

Correlates an authorized user with network resources



Connect to www.cisco.com

CCO

User name: student1

Password: ••••••••

☐ Remember my password

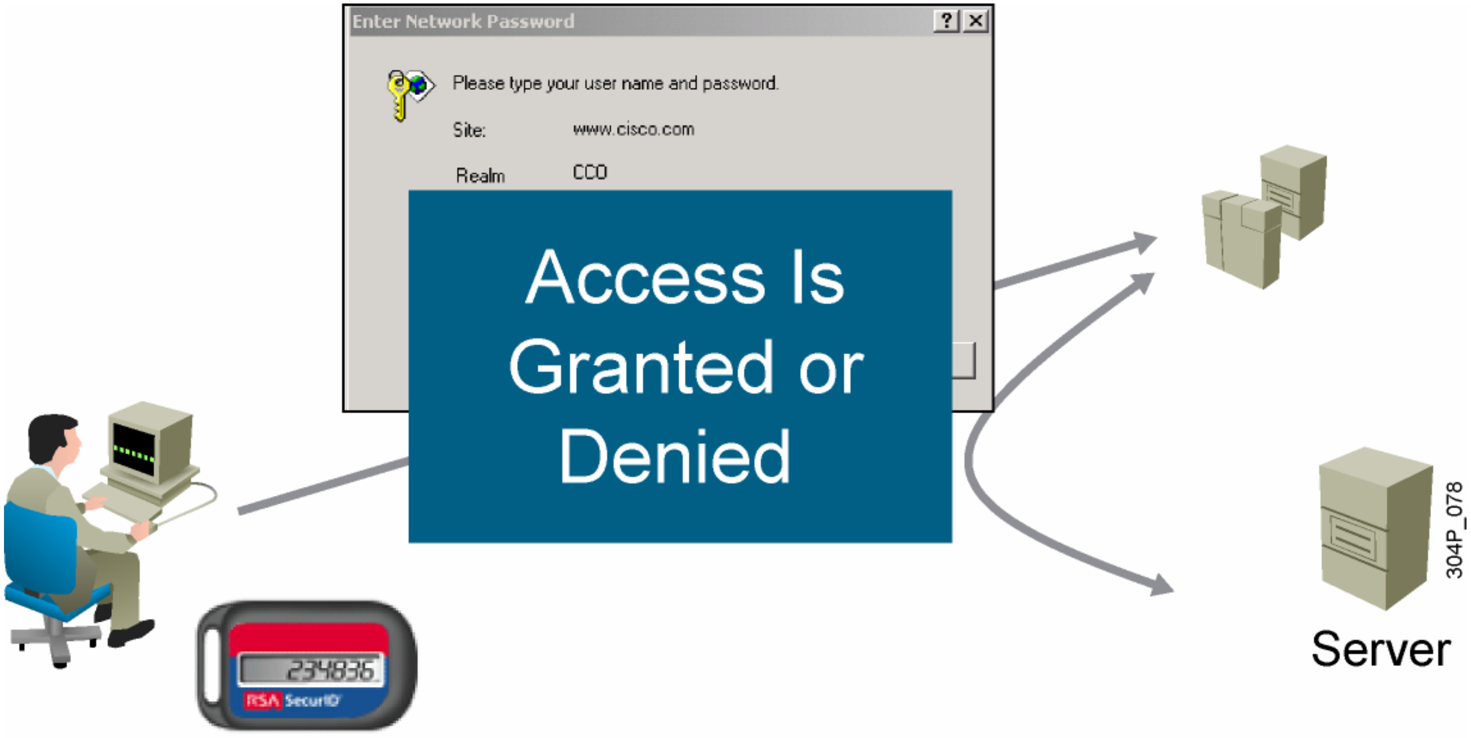
© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc, for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

Tokens

Strong (two-factor) authentication based on “something you know” and “something you have”



Enter Network Password

Please type your user name and password.

Site: www.cisco.com

Realm CCO

Access Is Granted or Denied

© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

www.CareerCert.info

Access Control in Networks

- Confidentiality and integrity are traditionally supported through access control.
- Access control enforces rules about which entities can access which resources.
- Network access control is based on:
  - Authentication, which establishes the identity of the subject
  - Authorization, which defines what a subject can do in a network
- Audit trails and real-time monitoring provide accounting and security auditing information.

© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

Example: Trust and Identity Management Technologies

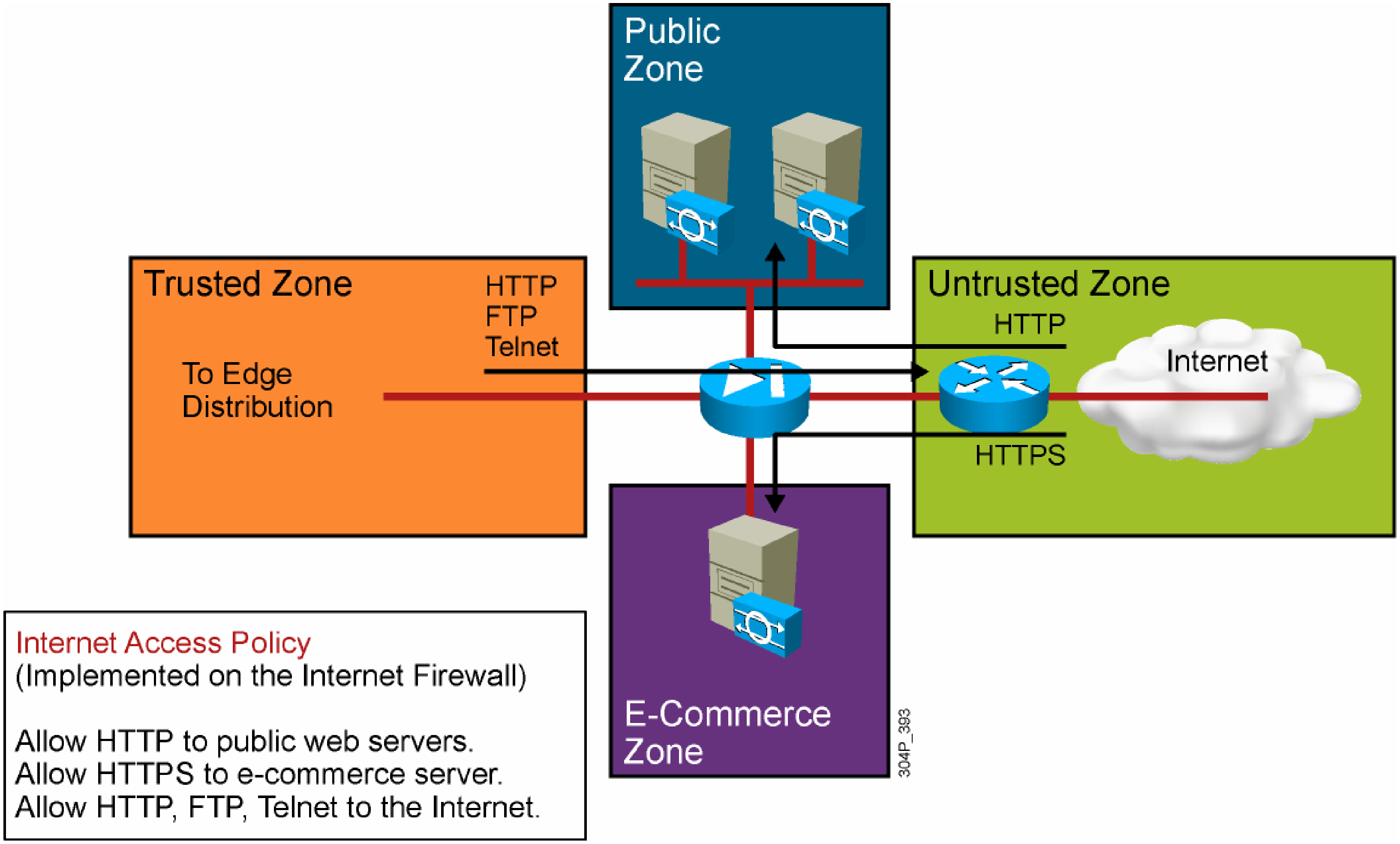
- Access control lists (ACLs)
- Firewalls
  - Stateful inspection
  - Application inspection
- Network Admission Control (NAC)
  - NAC Framework
  - Cisco NAC Appliance
- IEEE 802.1X
- Cisco IBNS

© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc. for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

Firewall Filtering Using ACLs



Internet Access Policy
(Implemented on the Internet Firewall)

Allow HTTP to public web servers.
Allow HTTPS to e-commerce server.
Allow HTTP, FTP, Telnet to the Internet.

© 2007 Cisco Systems, Inc. All rights reserved.

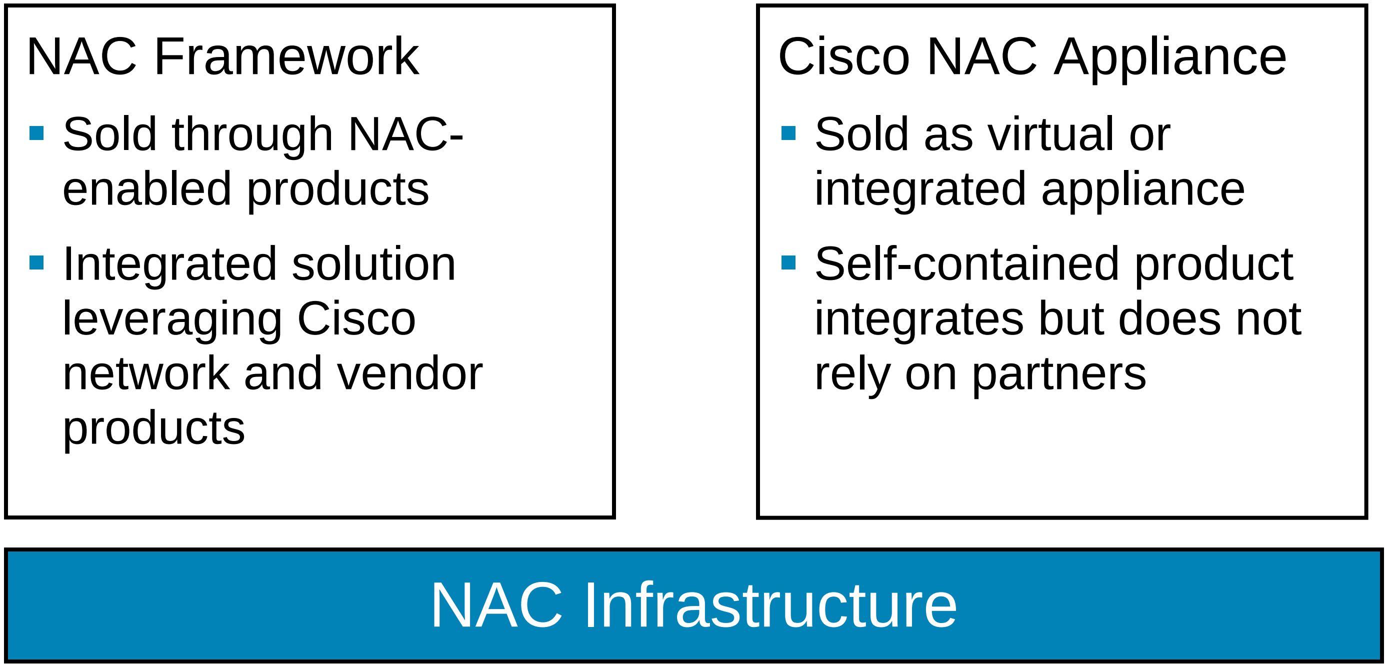
Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc. for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

www.CareerCert.info

NAC Framework and Appliance

Two approaches for Network Admission Control (NAC)



NAC Framework

- Sold through NAC-enabled products
- Integrated solution leveraging Cisco network and vendor products

Cisco NAC Appliance

- Sold as virtual or integrated appliance
- Self-contained product integrates but does not rely on partners

NAC Infrastructure

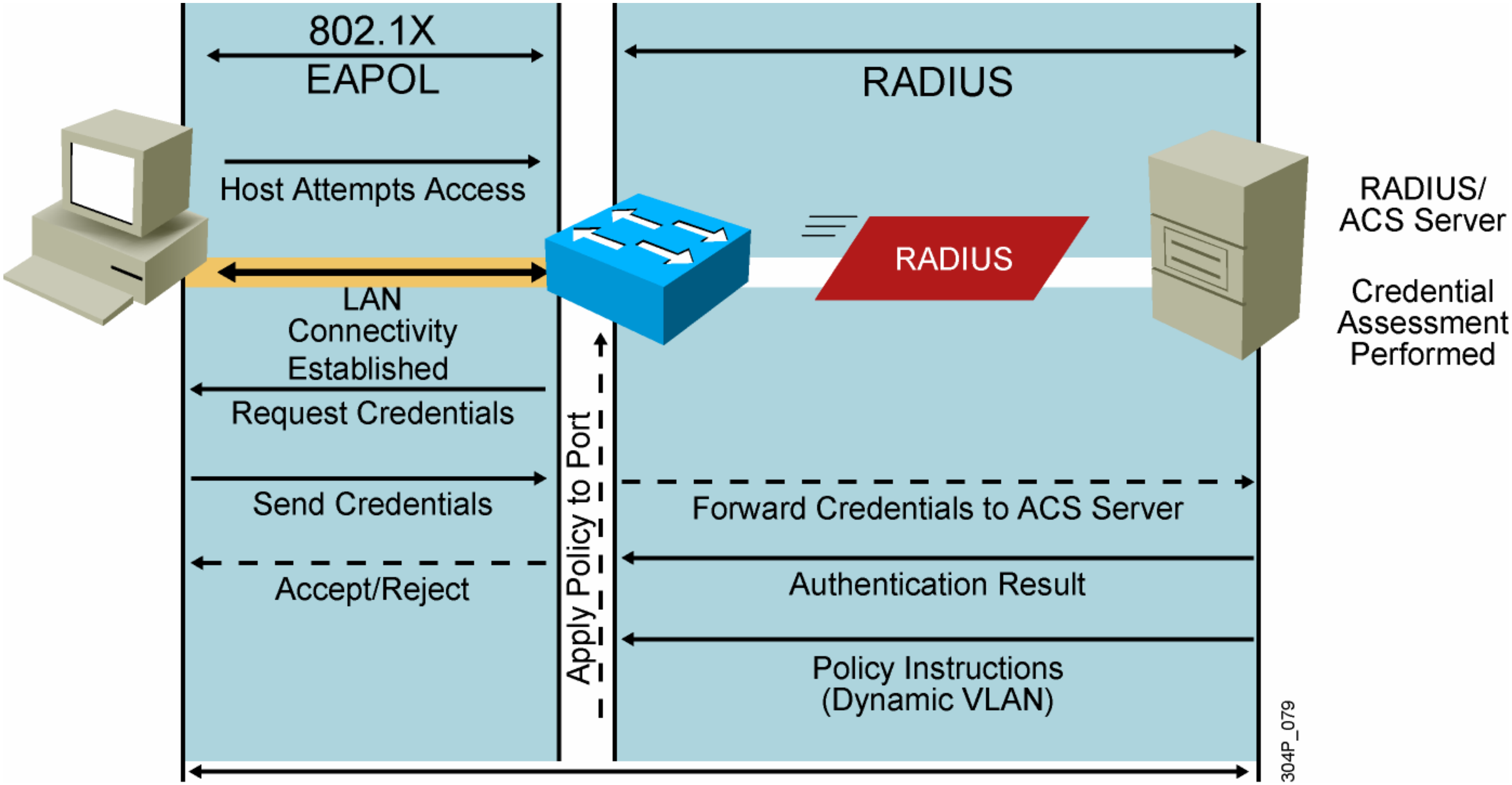
- Offers customers a deployment time-frame choice
- Adapts to investment protection requirements of customer

© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

802.1X Protocol



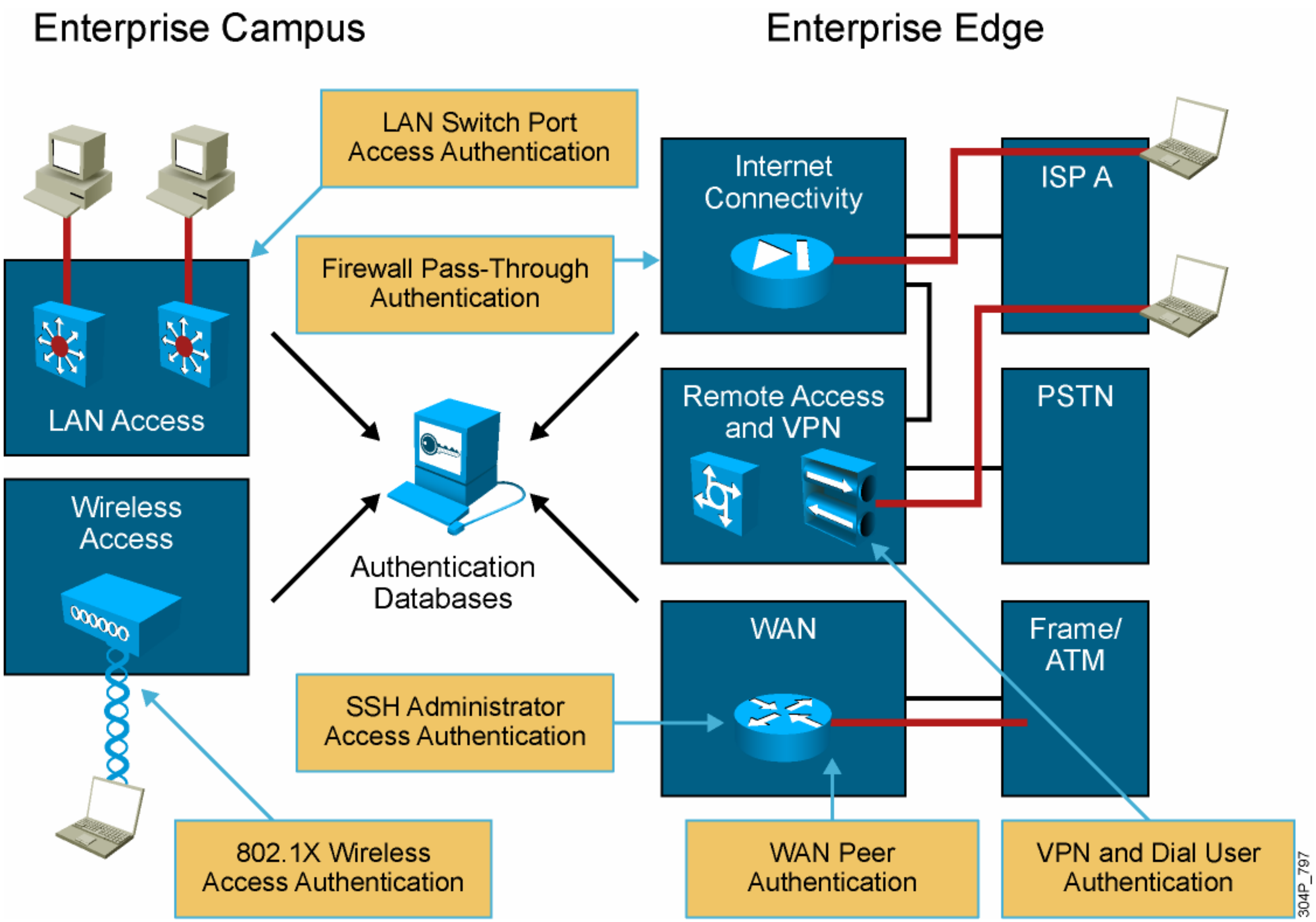
© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc.
for the sole use by Cisco employees for personal study. The files or printed representations may not be
used in commercial training, and may not be distributed for purposes other than individual self-study.*

Identity and Access Control Deployment Locations

- Authenticate at edge.
- Deploy ACLs based on policy.
- Practice defense in depth.



Enterprise Campus
Enterprise Edge
LAN Switch Port Access Authentication
Firewall Pass-Through Authentication
LAN Access
Wireless Access
Authentication Databases
SSH Administrator Access Authentication
802.1X Wireless Access Authentication
Internet Connectivity
Remote Access and VPN
WAN
ISP A
PSTN
Frame/ ATM
WAN Peer Authentication
VPN and Dial User Authentication
304P_797

© 2007 Cisco Systems, Inc. All rights reserved.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

Threat Defense

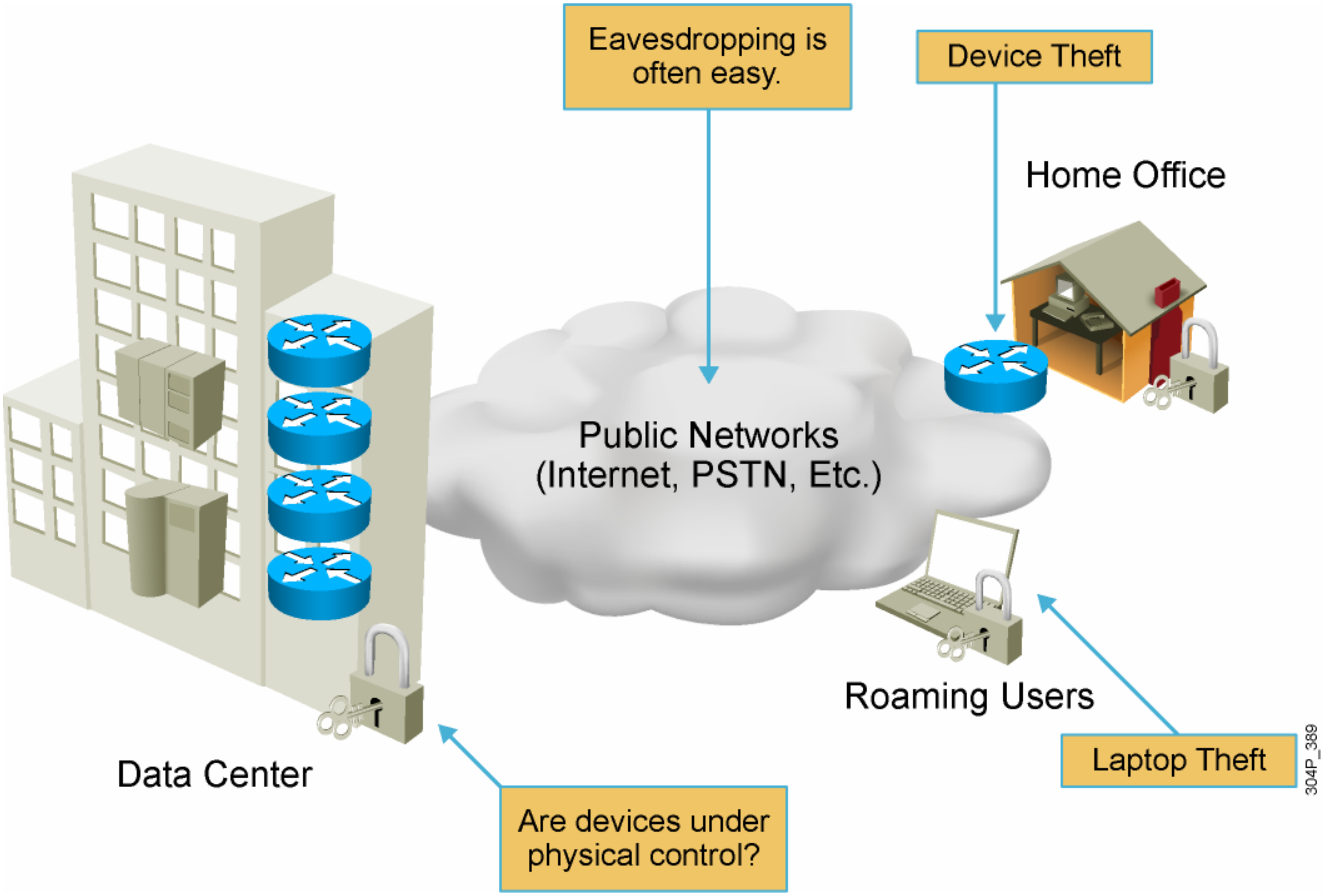
- Enhances security in the existing network infrastructure
  - Protects businesses from operation disruption, lost revenue, and loss of reputation.
- Adds comprehensive security on network endpoints
  - Cisco Security Agent provides endpoint protection.
- Adds dedicated security technologies to networking devices and appliances
  - Security technologies are implemented throughout the network.

© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc. for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

Physical Security


Eavesdropping is often easy.
Device Theft
Home Office
Public Networks (Internet, PSTN, Etc.)
Roaming Users
Laptop Theft
Data Center
Are devices under physical control?
304P_389

© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

www.CareerCert.info

Physical Security Guidelines

- Deploy adequate physical access control.
- Evaluate whether physical access can compromise other security features.
- Identify additional security issues resulting from device theft.
- Protect communications over infrastructure out of your control using cryptography.

© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc. for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

Infrastructure Protection

- The measures taken to preserve the integrity and availability of the network infrastructure as a transport and service entity
- Goals:
  - That the network devices are not accessed or altered in an unauthorized manner
  - That the end-to-end network transport and any integrated services remain available
- Policy enforcement technologies can help preserve, directly, the integrity and availability of the network.

© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc. for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

Infrastructure Protection Deployment Locations

- Deploy on all network infrastructure devices
  - Different mechanisms are used on different platforms, but typically there are equivalent functions available.
  - More advanced mechanisms are available mainly on higher-end platforms.
- Implement throughout the network

© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

www.CareerCert.info

Recommended Practices for Infrastructure Protection

- Use SSH to access devices.
- Enable AAA and role-based access control for access to all network devices.
- Collect and archive syslog information.
- Use SNMPv3.
- Disable unused services.
- Use SFTP (SSH FTP) or SCP and avoid FTP and TFTP.
- Install vty access lists to limit access to management and CLI services.
- Enable control plane protocol authentication.
- Consider one-step lockdown in SDM for basic router security.

© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc.,
for the sole use by Cisco employees for personal study. The files or printed representations may not be
used in commercial training, and may not be distributed for purposes other than individual self-study.*

www.CareerCert.info

Threat Detection and Mitigation

- Provide early detection and notification of unpredicted malicious traffic or behavior.
- Goals:
  - To detect, notify of, and help stop an event or traffic that is unauthorized and unpredicted
  - To help preserve the availability of the network, particularly against unknown or unforeseen attacks
- Technologies include:
  - Endpoint protection
  - Infection containment
  - Intrusion and anomaly detection
  - Application security and anti-X defense

© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

www.CareerCert.info

Example: Threat Detection and Mitigation Technologies

- Network-based intrusion prevention systems (NIPS)
  - Adaptive security appliance (ASA)
  - IPS sensor applicance
  - Cisco IOS IPS
- Host-based intrusion prevention systems (HIPS)
  - Cisco Security Agent
- NetFlow
- Syslog
- Event correlation systems
  - Cisco Security Monitoring, Analysis, and Response System (MARS)
- Cisco Traffic Anomaly Detector Module

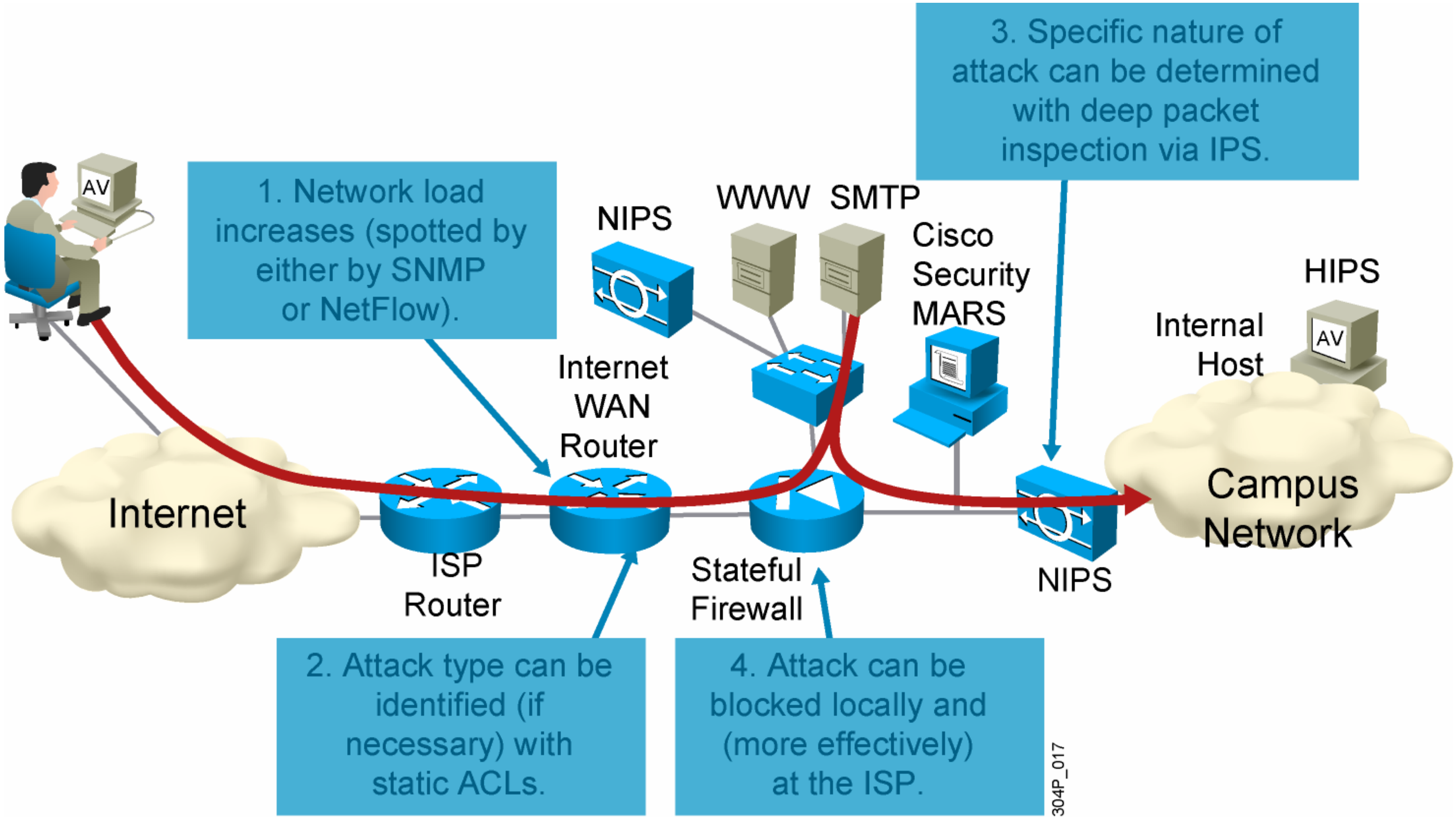
© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

www.CareerCert.info

Threat Detection and Mitigation Solutions Deployment Locations



1. Network load increases (spotted by either by SNMP or NetFlow).

2. Attack type can be identified (if necessary) with static ACLs.

3. Specific nature of attack can be determined with deep packet inspection via IPS.

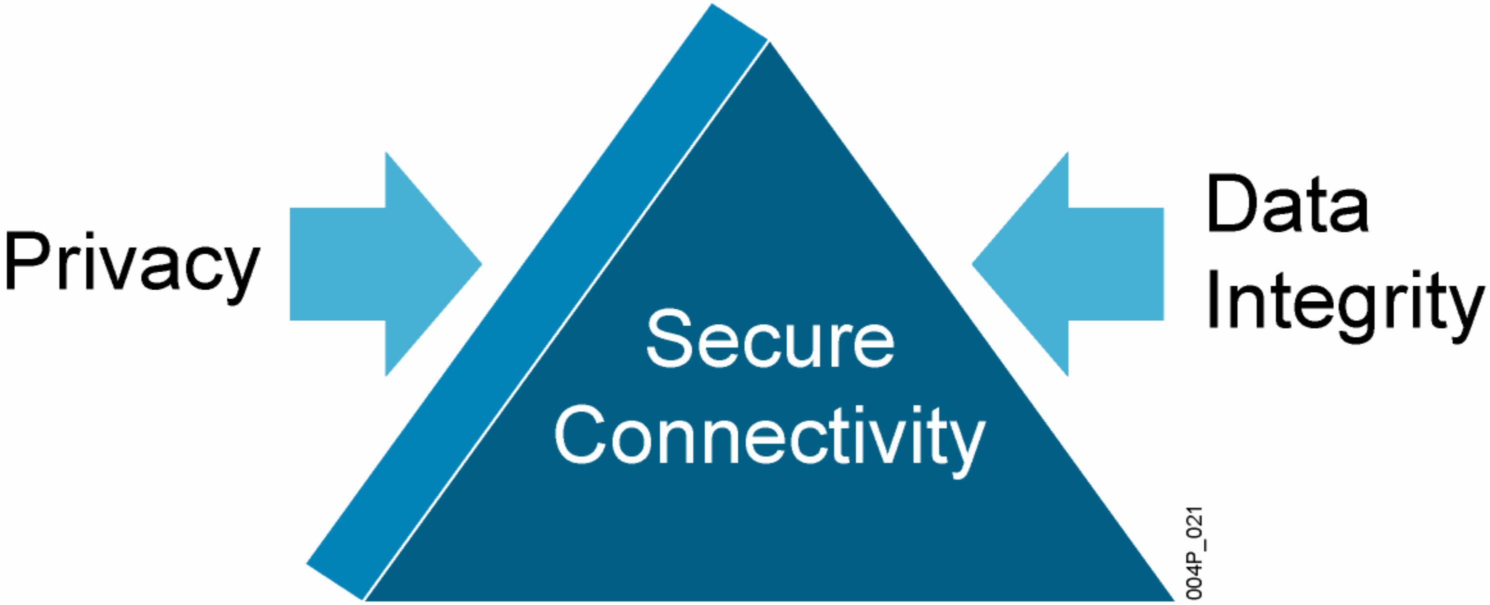
4. Attack can be blocked locally and (more effectively) at the ISP.

© 2007 Cisco Systems, Inc. All rights reserved.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

Secure Connectivity



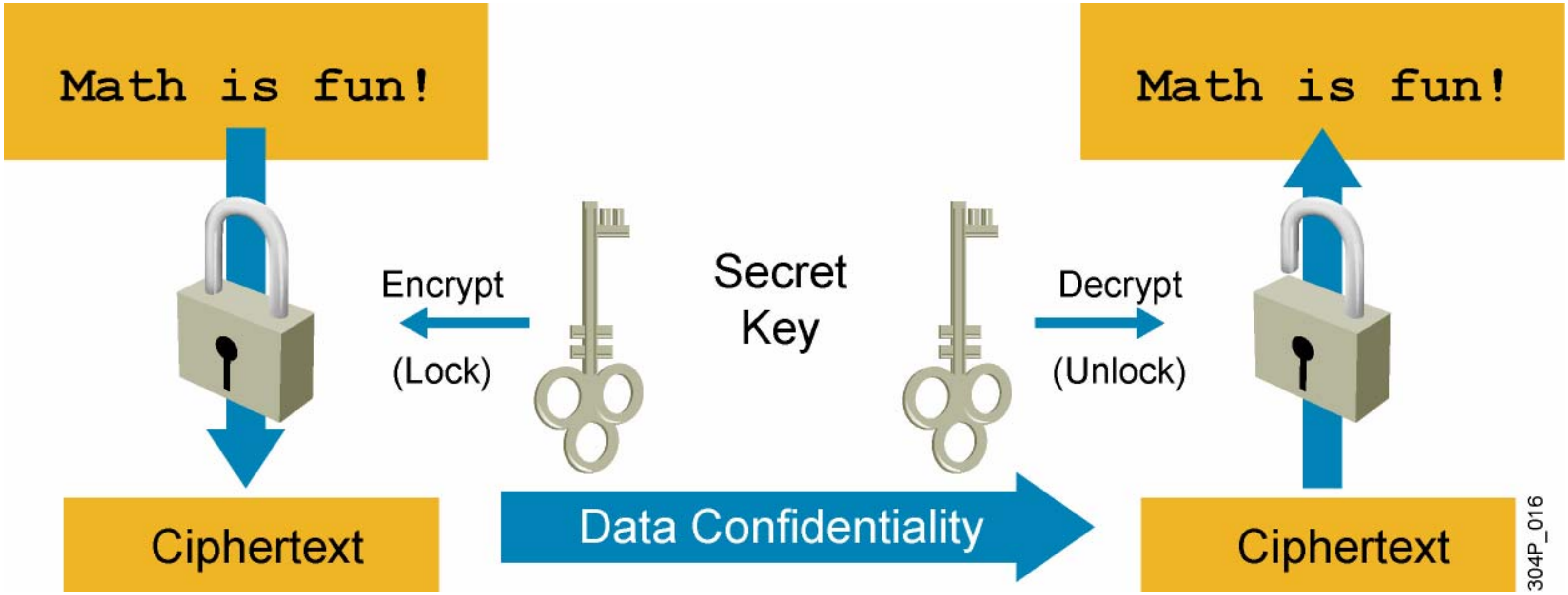
© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc. for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

Encryption Fundamentals

- A method of protecting the confidentiality of data
- Uses keys to encrypt the data and decrypt it at a later time



© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc. for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

www.CareerCert.info

Encryption Keys

Shared secrets:

- Secret key is carried “out of band” to the remote side.
- Easiest mechanism, but it has inherent security concerns.

Public key infrastructure (PKI):

- Uses “asymmetric cryptography” in which the encryption key is different from the decryption key
- Lets you publish the encryption key, while keeping the decryption key secret
- Widely used in e-commerce sites around the world

© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc. for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

VPN Protocols

IPsec (IP security)

- Built directly on the IP layer (Protocol 50)
- Uses IKE and ESP
- Requires IPsec software on endpoints

SSL (Secure Socket Layer)

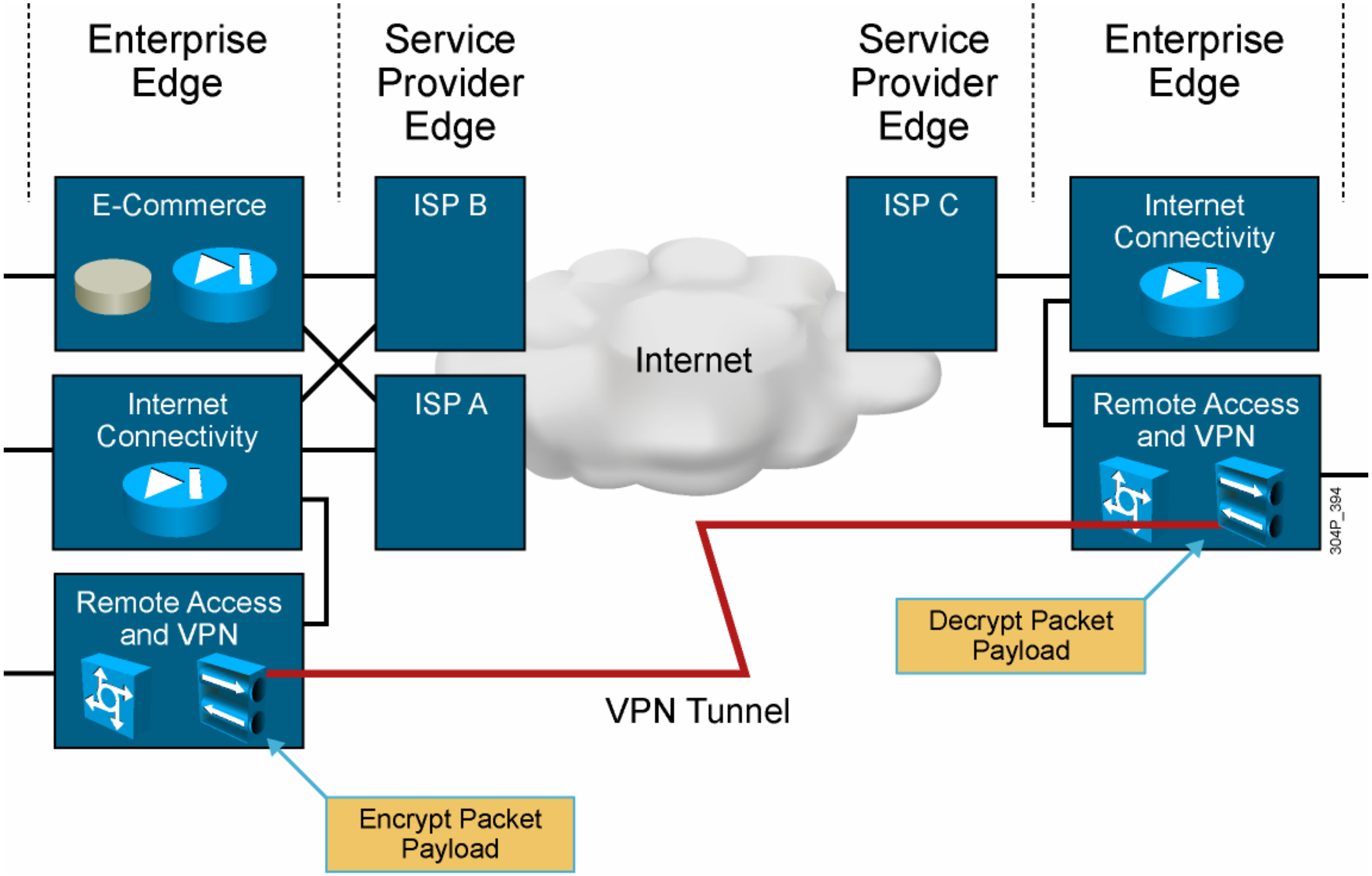
- Built on top of the TCP layer (port 443)
- Provides confidentiality for web traffic (HTTPS)
- All major browsers can use SSL

© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc. for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

Transmission Confidentiality



© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

www.CareerCert.info

Transmission Confidentiality Guidelines

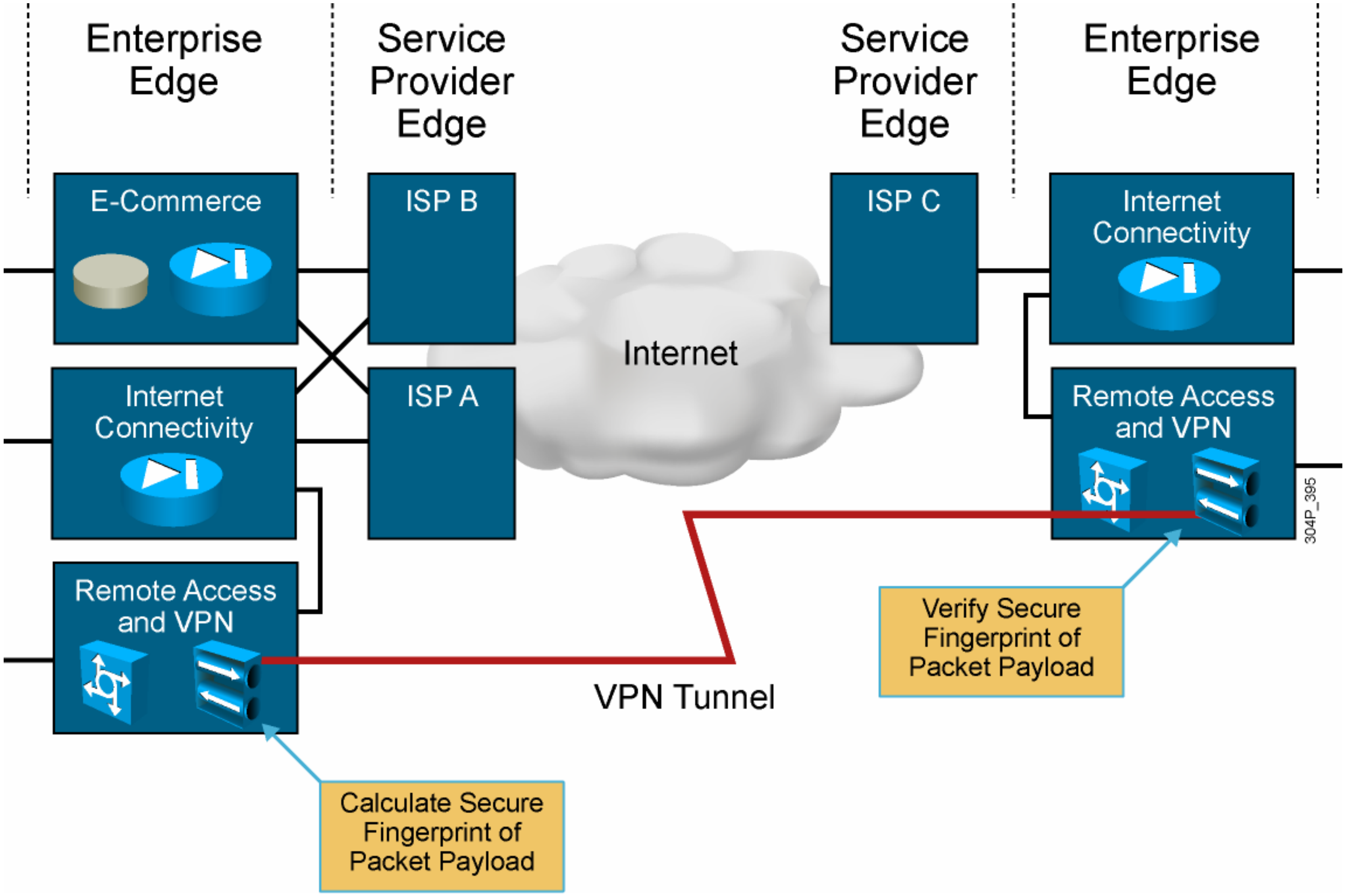
- Evaluate the location for transmission confidentiality needs.
- Use the strongest available cryptography, performance permitting.
- Use well-known and established cryptographic algorithms.
- Do not focus on confidentiality alone; integrity and authenticity are also important.

© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc. for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

Data Integrity



Verify Secure Fingerprint of Packet Payload

Calculate Secure Fingerprint of Packet Payload

© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc. for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

www.CareerCert.info

Data Integrity Guidelines

- Evaluate the need for transmission integrity.
- Use the strongest available cryptography, performance permitting.
- Use well-known and established cryptographic algorithms.

© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc. for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

www.CareerCert.info

Security Management Overview

- Security management does the following:
  - Collects, analyzes, and presents data
  - Provisions policies on security devices
  - Maintains consistency and change control of policies
  - Provides role-based access control and accounts for all user activity
- Security implementation is only as good as policies used.
- Biggest risk to security in a properly planned architecture is policy error.

© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

www.CareerCert.info

Security Management Solutions

- Cisco Router and Security Device Manager (SDM)
- Cisco Adaptive Security Device Manager (ASDM)
- Cisco Intrusion Prevention System Device Manager (IDM)
- Management Center for Cisco Security Agents
- Cisco Secure Access Control Server (ACS)
- Cisco Security Manager
- Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS)

© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

Summary

- The Cisco Self-Defending Network integrates security into the network to provide the network the ability to identify, prevent, and adapt to threats.
- Trust and identity management provide secure network access and admission at any point in the network and isolate and control infected or unpatched devices that attempt to access the network.
- Threat defense provides a strong defense against known and unknown attacks using security integrated in routers, switches, and appliances.
- Secure connectivity uses encryption and authentication to provide secure transport across untrusted networks.
- Security management is a framework for scalable policy administration and enforcement.

© 2007 Cisco Systems, Inc. All rights reserved.

Please purchase PDF Split-Merge on www.verypdf.com to remove this watermark.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc. for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.