1..routing protocol authentication..1

2..Local AAA authentication provides a way to configure backup methods of ..2authentication, but login local does not…2

3..The authentication process stops. [*adef*]..3

4..identification of Layer 3 protocol support on hosts

4..TCP and UDP port scanning [*adef*]

5..retired false

6..They produce identical subkeys.

7..granularity control within applications

8..The Cisco IOS image file is not visible in the output of the show flash command.

9..split tunneling

10..The ASAs must all be running the same ASDM version.

10..ASDM must be run as a local application.

11..ISAKMP SA policy

12..The ZPF is not dependent on ACLs.

12..ZPF policies are easy to read and troubleshoot.

13..required steps to ensure consistent configuration of all company switches

14..HMAC

15..an uplink port to another switch

16..A router interface can belong to only one zone at a time.

 17..The password cisco123 is wrong.

18..MAC and IP address spoofing [*adef*]

 19..The crypto map has not yet been applied to an interface. [*Gilardi*]

20..symmetric algorithms [*original answer*]

21..Packet filters perform almost all the tasks of a high-end firewall at a fraction of the cost.

22..aaa accounting exec start-stop group tacacs+

23..allows a Cisco ACS server to minimize delay by establishing persistent TCP connections [*adef*]

24..Keep a secure copy of router operating system images.

24..Configure the router with the maximum amount of memory possible.

25..It uses UDP port 500 to exchange IKE information between the security gateways.

26..209.165.201.1

27..Traffic that is sent from the DMZ and the LAN to the Internet is considered outbound.

28..The code has not been modified since it left the software publisher.

28..The code is authentic and is actually sourced by the publisher.

29..VLAN ID

30..uses connection information maintained in a state table

30..analyzes traffic at Layers 3, 4 and 5 of the OSI model

31..can be implemented as software or as a service

31..examines logs and events from systems and applications to detect security threats [*adef*]

31..consolidates duplicate event data to minimize the volume of gathered data

32..inside to DMZ [*adef*]

33..signature-based [*adef*]

34..reset TCP connection

34..alert

34..drop

 35..SSL

36..A single CLI view can be shared within multiple superviews. [*adef*]

38..A class 5 certificate is more trustworthy than a class 4 certificate. [*adef*]

39..The hosts that are identified in the ACL will have access to the device.

40..Use a web browser to visit the destination website.

41..The user can issue the show version command.

42..stateful packet inspection [*John / adef*]

 43..ISR router

43..another ASA

44..VLAN hopping

45..authorization

46..An alert is triggered each time a signature is detected. [*adef*]

47..AES [*John / adef*]

47..SHA [*John / adef*]

 49..It is virtually impossible for two different sets of data to calculate the same hash output. [*adef*]

50..integrity checker

51..This message is a level five notification message.

51..This message indicates that service timestamps have been globally enabled.

52..Both VPN end devices must be NAT-T capable.

53..This port is currently up. [*adef*]

53..Security violations will cause this port to shut down immediately.

53..The switch port mode for this interface is access mode. [*adef*]

54..traffic originating from the DMZ network going to the inside network

54..traffic originating from the outside network going to the inside network

 55..Only signatures in the ios\_ips basic category will be compiled into memory for scanning.

 56..promiscuous ports

56..community ports belonging to the same community

57..It encrypts the entire body of the packet for more secure communications.

58..Implement encryption for sensitive traffic. [*adef*]

 59..NIPS monitors network segments.

 60..Disable both protocols on all interfaces where they are not required.

 61..security policy compliance

62..binding class maps with actions

63..exec

65..A local username database provides redundancy if ACS servers become unreachable. [*adef*]

66..Traffic from the LAN and DMZ can access the Internet.

 67..to prevent data traffic from being redirected and then discarded

67..to prevent redirection of data traffic to an insecure link

 68..required steps when reporting a breach of security

69..Adaptive Security Appliance

70..BPDU guard

70..PortFast

 71..Email viruses are the most common type of them.

 72..SDEE notification is disabled by default. It does not receive and process events from the Cisco IOS IPS unless SDEE notification is enabled.

73..L0phtcrack

74..Administrators can decide what actions can be taken in the future.

75..Enable DAI on the management VLAN.

76..RADIUS

77..show xlate [*jack*]

78..acceptable use policy

78..remote access policy

78..network access policy

79..governing policy

 80..Configure SSH.

84..redundant ISP connections

83..Hairpinning

84..Commands from a lower level are always executable at a higher level.  
84..AAA must be enabled.

85..vulnerability brokers  
85..hacktivists

86..VLAN 2  
87..accounting  
88..the lowest bridge ID

89..to encapsulate multiple OSI Layer 3 protocol packet types inside an IP tunnel

90..the layer 2 address with the lowest hexadecimal value