Video 1

SDM - Security Device Manager
One Step Lockdown
SDM Security Audit
Authentication, Authorization, Accounting

Day 1 - setting up SDM and TACACS+/RADIUS
Day 2 ACLs for once AAA is set up

Mitigating attacks on Layer 2 - Catalyst switches, etc
mentioned attack - RAM depletion/ buffer overflow, DHCP server impersonation

Turning a router into a firewall with SDM
CBAC - content based access control

Day 3 - IPSEC tunnels, setting up with SDM

Smurf is ICMP echo request, Fraggle is UDP echo
TCP RST attack on BGP - source spoof router IP to add/delete - RST will reset routing tables for given route

TCP window as relating to range of sequence numbers
Blind vs non-blind spoofing - refers to if attacker can see traffic or not (for things like sequence numbers) - Session hijacking - solution IPSEC or SSL/TLS
TCP RST attacks on BGP are generally blind- session termination attack - won't know sequence numbers
Solution to BGP attack is passwords between neighbors

Since there are many ways to implement spoofing for different purposes, there are different ways to mitigate it
- Access Control Lists (ACLs)
  - RFC 2827 – "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing"
- Unicast Reverse Path Forwarding (URPF)
- ARP Inspection
- DHCP Snooping
- IP Source Guard
- Routing Protocol Authentication
- BGP TTL Security
- IP Options checking (source routing)
- IPsec VPNs

If source routing is on on an IP packet, you generally want those packets dropped. It isn't used for legitimate purposes anymore

Video 3
Recon attacks - network mapping attacks (routers, links, routing tables, hosts, firewalls, etc)
Sniffing
Ping sweep for enumeration
Port scans on found IPs
DNS queries to root DNS servers to find breadcrumbs to other servers (like SQL servers registered via DNS)

ICMP echo, unreachable, mask reply (I know the IP address, what is your interface's subnet mask?), redirect
[**redirect** is compared to split horizon, where we don't send a routing update back out the interface it came from. ICMP reply says back, "don't use me for routing to this IP- use this instead. I am using this same interface to reach that IP" - this can be used to see what the routing table looks like. Route unreachable means it isn't in the routing table]
Proxy ARP (see later, layer 2 attacks)
CDP - recommended to turn it off- however phones use CDP
Mitigate by disabling unneeded services, employing IPS to match signatures of scans

Control Plane attacks - disrupt routing and management protocols - network DOS attack
Packet injection/withdrawl
BGP reset
telnet passwords
SNMP community strings
NTP spoofing

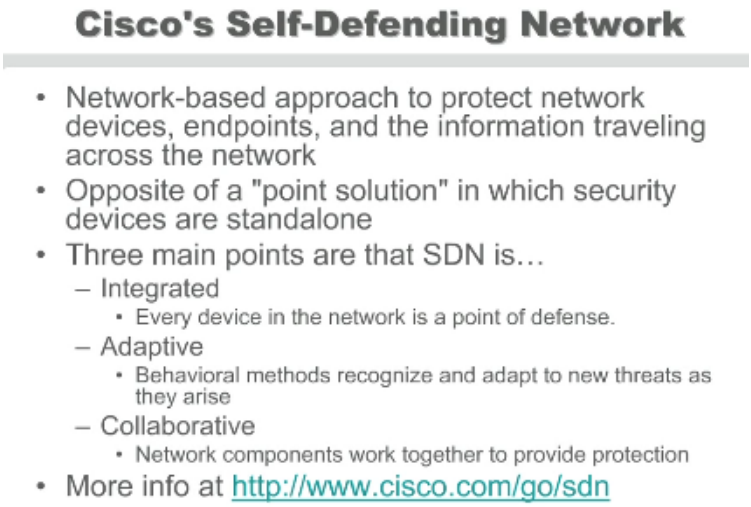
Vulnerabilities and mitigations:
No routing authentication - make sure the routing tables-exchange uses passwords or hashes
Promiscuous routing neighbors - use unicast updates (You can even get really granular and say only this MAC address can send me packets)
Clear text telnet, SNMP, etc passwords (use SSH, SNMPv3, etc)
No NTP authentication

DoS - ip spoofing,
smurf, fraggle - flood amplification prevention - put "no ip redirect" on your routers
TCP SYN flooding
Creating tons of half-open TCP connections reaching TCP stack connection limits
Upper layers like Apache can also have limits
Input packets not RPF-checked - have a firewall proxy to monitor/set/enforce thresholds
Spoofing prevention: RFC 2827/ BOGON filtering / URPF. If packet coming in with invalid address, drop it, especially private address space in source address coming from public address space

Access attacks - brute force/ keyloggers/ packet sniffers/ layer 3 MitM/ redirection
Mitigation: AAA/ lockouts, SSL/IPSec/ HIPS, good passwords, no cleartext, turn off any redirection capability

Network Access Control (NAC) Cisco says "Admission control"

This is more of a marketing thing, but is something that likely comes up on Cisco exams:



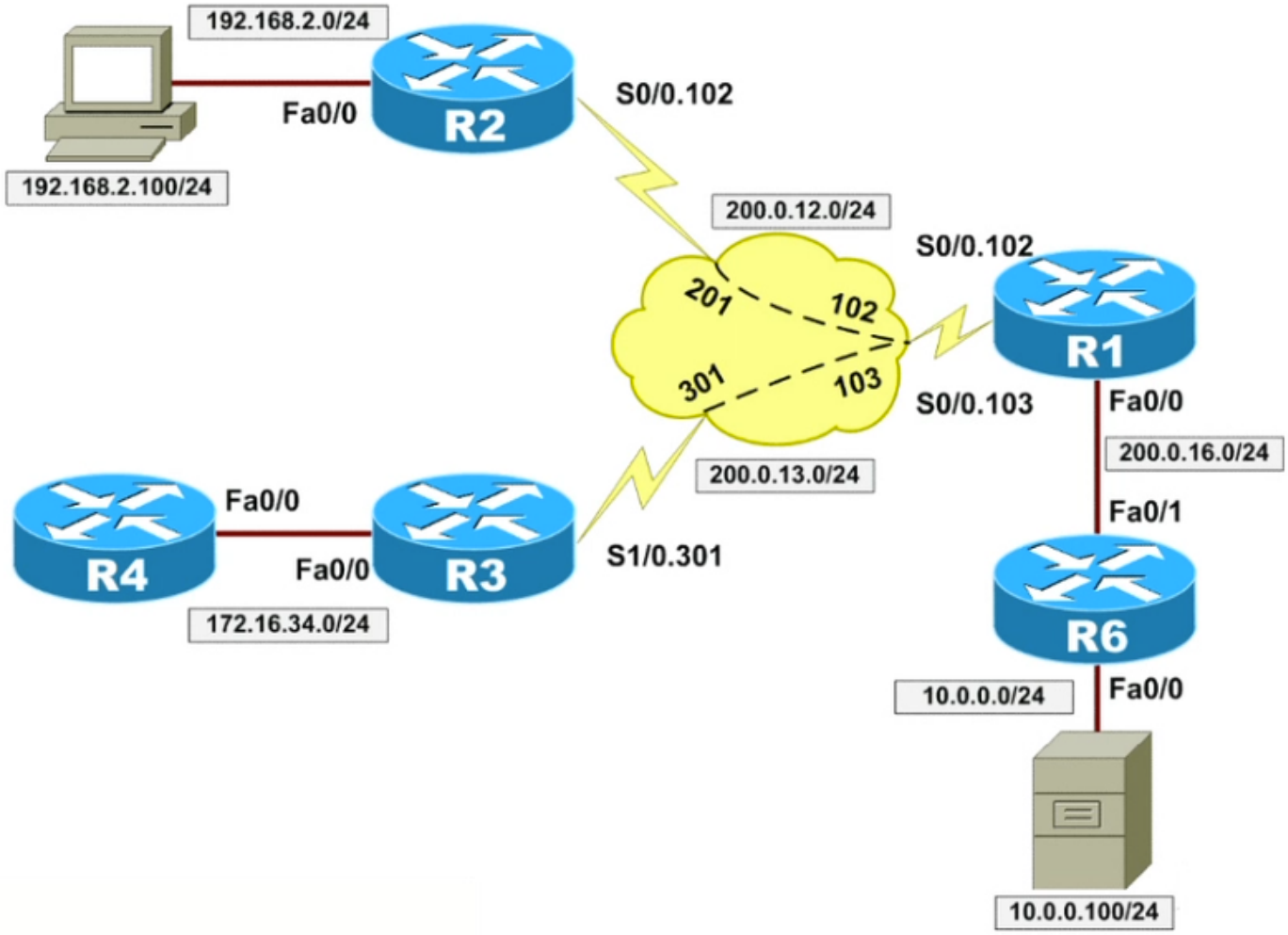
Basically, it means all of the portions of the network are working together as a security suite

Recommended list to get on:
Cisco Product Security Incident Response Team (PSIRT) signup at www.cisco.com/security/

SDM Security Audit feature to automatically identify common misconfigurations (with best practices)
One-step Lockdown automatically fixes found issues. Not as thorough- not good for non-standard setups.
Optionally, manually use checkboxes in SDM to make changes (recommended)
It is recommended to make changes in a sandbox, the check over changes at CLI before applying them to production devices

Note: the term deferred version or deferral in IOS terms means something has been fixed and it needs to be upgraded- there are no updates like a host OS- you have to reinstall the entire OS image

Basic lab configuration:



- R6 border router connecting to unsecure network - has web service enabled, local authentication, username/pass, for SDM (ip http server)
- R1, 2, 3, 4 other devices on internet.
- Host 10.0.0.100/24 - used for Cisco ACS, testbed for RADIUS and TACACS+. Launching point for SDM Visit that host in browser, login.

It is explained that it is the EXEC process that you are logging into, meaning to manage the router. Normally, browsing a webpage is not the EXEC process. It is explained this will come up later
Passwords - are of Type 0 5 and 7. 0 is least secure (cleartext)
enable password cisco- thats type 0. Type 5 is username secret/ enable secret - md5 one-way hash in running config Type 7 was Cisco's first attempt at security/ encryption... is reversable. All you have to do is run it through type 7 encryption backward- was never meant to be secure encryption. Is mainly to prevent shoulder-surfing.
service password-encryption and in running config it will also have enable password 7a23ce323
tip: **security password min-length** to enforce policy
R6(config) # key chain 1
R6(config- keychain) # key 1
R6(config- keychain-key) # key-string 7 7a23ce323
R6(config- keychain-key) # end
R6# show key chain
Key-chain 1:
key 1 -- text cisco

```
R6(config)#enable secret cisco
The enable secret you have chosen is the same as your enable password.
This is not recommended.  Re-enter the enable secret.

R6(config)#no enable password
R6(config)#enable secret cisco
R6(config)#end
```

Type 5 like this is recommended - username tristan secret cisco -

Don't forget to set exec-timeout (seconds) not 0, which means never logout
Disabling password recovery
3 ways to recover - console or aux port and remote management
Console should always be available
Reboot, break, confreg it 4202
***"no service-password security"** - where physical security is an issue. Doesn't disable recovery - VERY important-*
This makes the router DELETE ITS CONFIG FROM NVRAM when it goes into ROMMON
This is a hidden command, meaning it will not show up when typing "no service?"

Note: Cisco equip makes no distinction between wrong username or wrong password (brute force deterent)

Deterring brute forcing EXEC process with IOS login enhancements

- Even with strong password policy, brute force attack on login is still possible
  - Login enhancements deter this, and add visibility through logging
- Accomplished through…
  - Delaying the login prompt after failure
    - `login delay seconds`
  - Blocking login prompt after failure
    - `login block-for seconds attempts tries within seconds`
  - Generating log message on success or failure
    - `login on-failure log [every login]`
    - `login on-success log [every login]`
  - Still permitting authorized stations
    - `login quiet-mode access-class {acl-name | acl-number}`

Video 5
Once authenticated, local command authorization assigned by levels (access to EXEC commands)
Default privilege levels: 0 (none), 1 (user mode), 15 (privilege/enable mode; higher number includes levels beneath
Running "enable" and "enable 15" are basically the same.
Levels 2-14 available for assignment, but there are better ways of doing that and it isn't recommended
Role-based CLI and remote command authorization make it much simpler
"show parser dump ?" echoes EVERY command available at current level you would be able to access with "?"
"show parser dump interface" echoes all interface commands available
Echo privilege mode you are in with "show privilege"
Recall that just adding plain "login" to console, aux, or vty will only ask for password, not authentication as username
"login local" means login checking local DB on device

- Privilege level can be assigned with globally, per user, or per line
- Globally
  - `enable password cisco`
    - Grants privilege level 15
  - `enable password level 2 cisco2`
    - Grants privilege level 2
- Per user
  - `username bob privilege 2 password cisco`
    - Grants privilege level 2
- Per line
  - `Router(config)#line vty 0 4`
  - `Router(config-line)#privilege level 15`
    - Grants privilege level 15 to all telnet users

Assigning privilege levels to line is NOT a good practice! You need to require username, password for precise authentication and authorization

If not authorized to use a command, the typical message is: **% Invalid input detected at the '^' marker.**
(meaning it won't say that's the reason, it is that to this mode, IOS is ignorant the command even exists!)

Assigning which levels can access what command.
Below are only 3 modes, but there are hundreds. This is why it is not a helpful way of doing this. There are also tons of esoteric and deprecated commands in IOS never used. There are also some complications, such as being able to assign permissions to an interface command, but not allowing the custome level to use config t to get to interface mode! It can get convoluted so it isn't recommended.

- Level can be modified down or up to grant or revoke user's access to a certain command
  - **privilege *mode* [all] {level *level* | reset} *command-string***
- Mode determines where the command exists in the CLI hierarchy
  - "exec" command
    - **router#**
  - "configure" command
    - **router(config)#**
  - "interface" command
    - **router(config-if)#**

The alternative is Role-based CLI
Provides users with "views" which control what can and can't be run (allows explicit denies on specific commands)
Superviews can be put together from multiple views, with some hierarchical grouping

R1(config)# username bob pass cisco
R1(config)# aaa new-model
R1(config)# aaa authentication login LOCAL1 local
R1(config)# line con 0
R1(config-line)# login authentication LOCAL1

R1(config)# parser view VIEWA
R1(config)# exit
R1# enable view
password:
R1# config t
R1(config)# parser view VIEWA
R1(config-view)# password cisco <--- add password to the view

username bob2 password cisco
username bob2 view VIEWA
username bob2 privilege 15

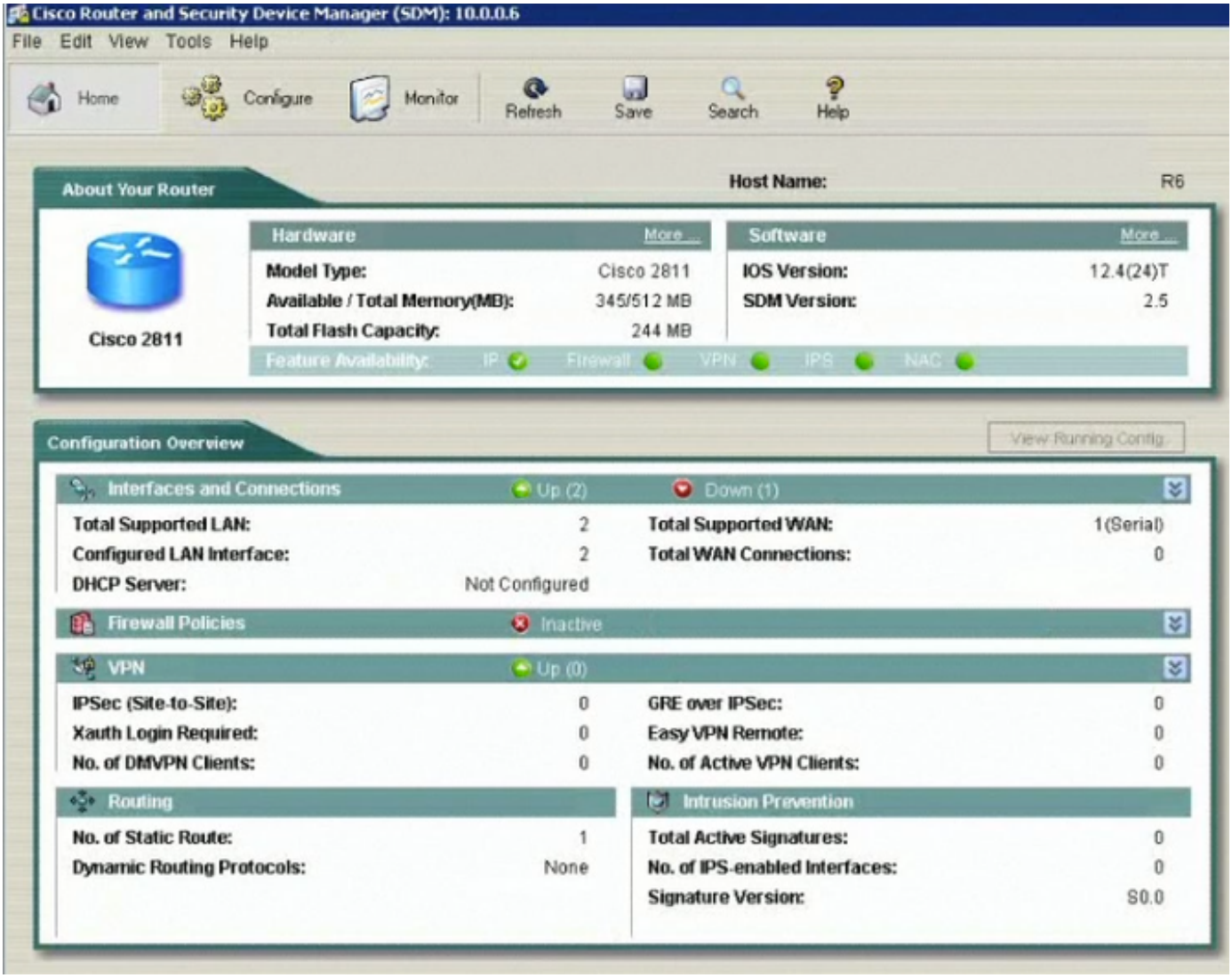
```
R1(config-view)#secret cisco
R1(config-view)#?
View commands:
  commands  Configure commands for a view
  default   Set a command to its defaults
  exit      Exit from view configuration mode
  no        Negate a command or set its defaults
  secret    Set a secret for the current view
R1(config-view)#commands ?
  RMI-Node-Config             Resource Policy Node Config mode
  RMI-Resource-Group          Resource Group Config mode
  RMI-Resource-Manager        Resource Manager Config mode
  RMI-Resource-Policy         Resource Policy Config mode
  SASL-profile                SASL profile configuration mode
  aaa-attr-list               AAA attribute list config mode
  aaa-user                    AAA user definition
  accept-dialin               VPDN group accept dialin configurati
  accept-dialout              VPDN group accept dialout configuraton mode
  address-family              Address Family configuration mode   ion mode
  aic         mily            Alarm Interface Card configuration m
  archive                     Archive the router configuration modode
  bba-group                   BBA Group configuration mode        e
  boomerang                   Boomerang configuration mode
  cascustom                   Cas custom configuration mode
  cns-connect-config          CNS Connect Info Mode
  cns-connect-intf-config     CNS Connect Intf Info Mode
  cns-tmpl-connect-config     CNS Template Connect Info Mode
  cns_inventory_submode       CNS Inventory SubMode
  config-ip-sla-http-rr       IP SLAs HTTP raw request Configuration
  config-l2tp-class           l2tp-class configuration mode
  config-saa-http-rr          SAA HTTP raw request Configuration
R1(config-view)#commands exec ?
  exclude             Exclude the command from the view
  include             Add command to the view
  include-exclusive   Include in this view but exclude from others
R1(config-view)#commands exec exclude ?
  LINE  Keywords of the command
  all   wild card support
R1(config-view)#commands exec exclude show ip route
```

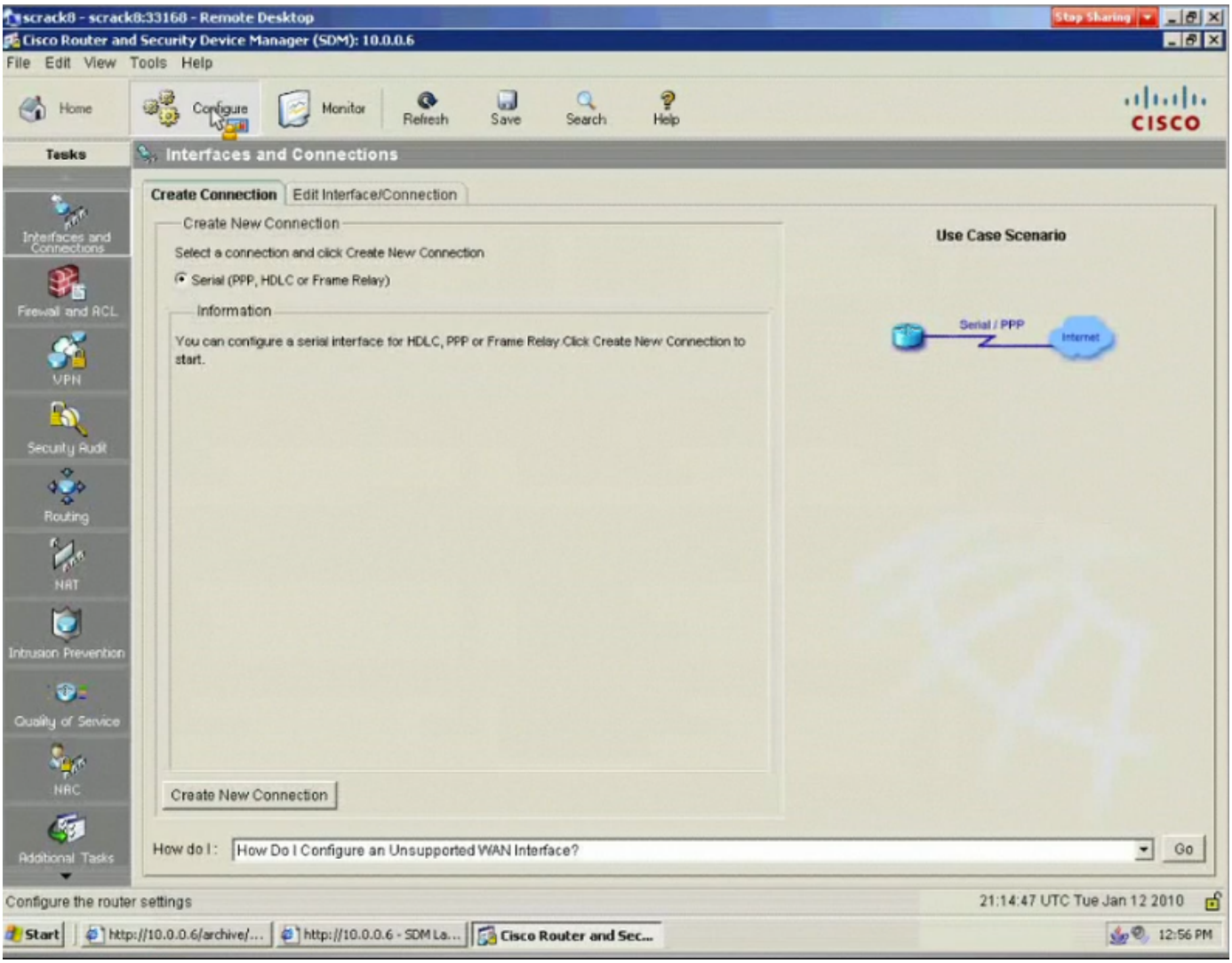
<u>Here is what we see in sh running config:</u>

```
!
control-plane
!
!
!
line con 0
 logging synchronous level 0 limit 20
 login authentication LOCAL1
line aux 0
line vty 0 3
line vty 4
parser view VIEWA
 secret 5 $1$jHOL$1NVU4OeGkEi.8VNw6rdVw0
 commands exec exclude show ip route
 commands exec include show ip
 commands exec include show
!
```

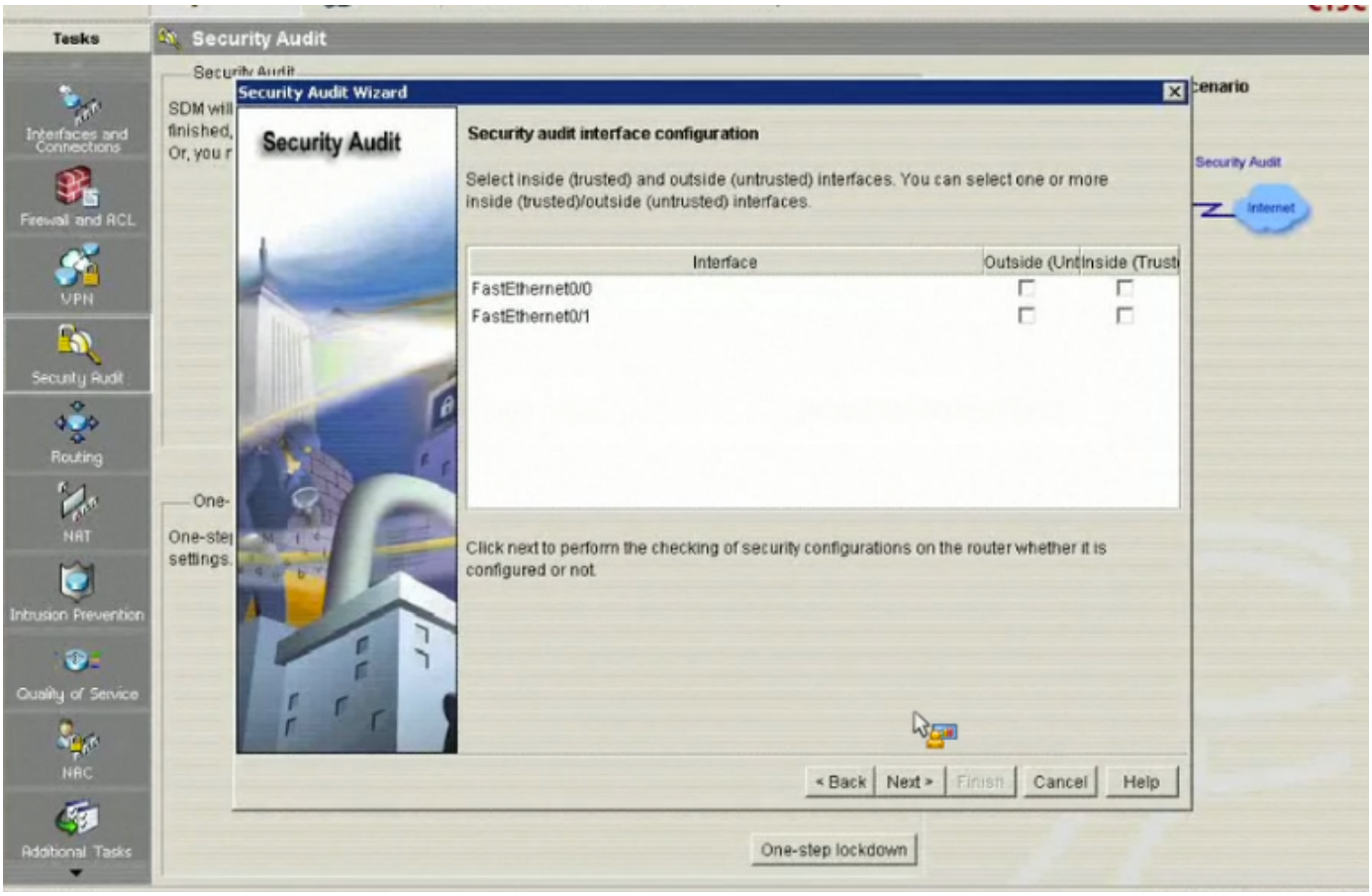
"command exec include-exclusive show ip int brief" means only that view it is applied to can (exclusively) run that command, and others will be disallowed.

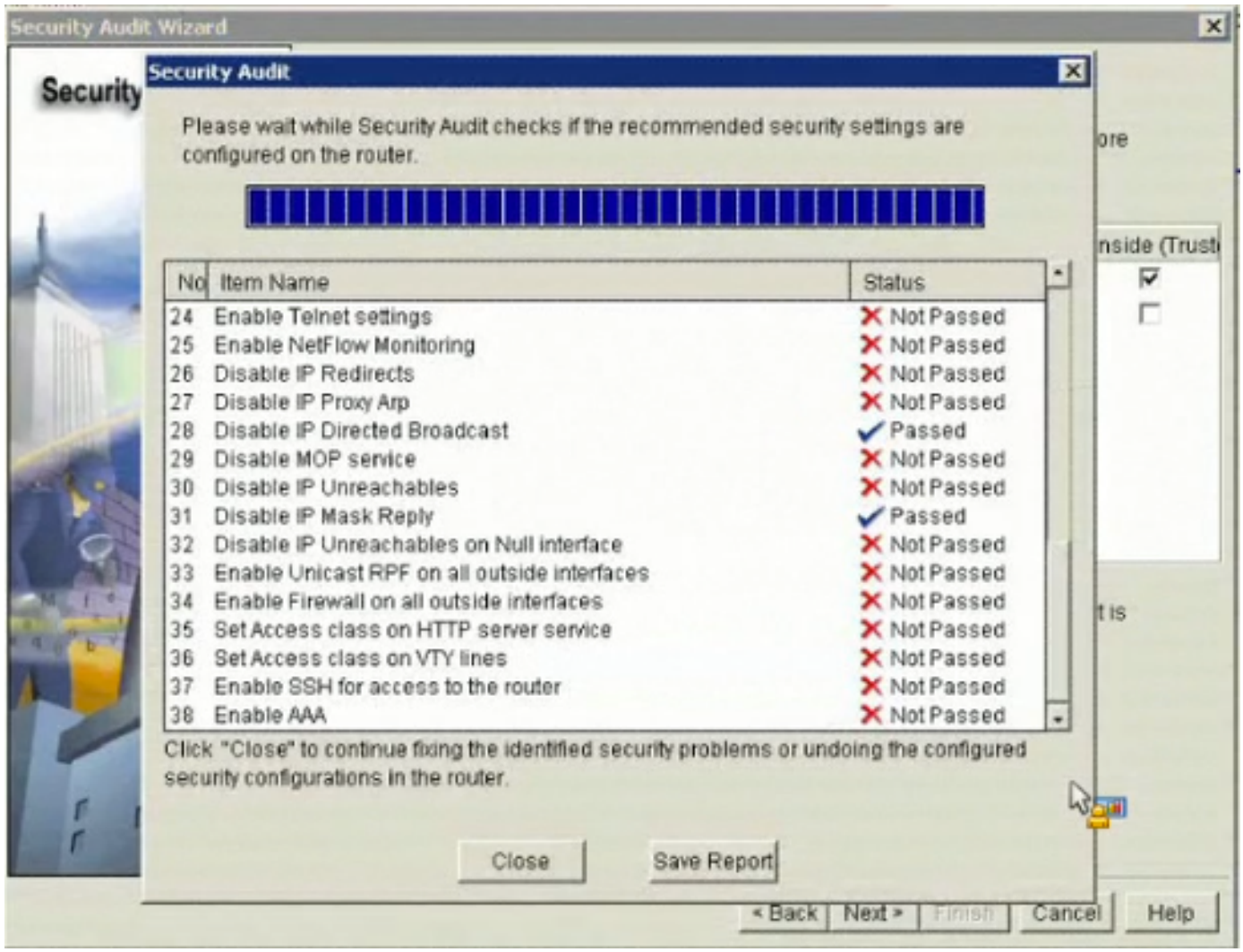
Security Device Manager pics below were in video 2 or 3

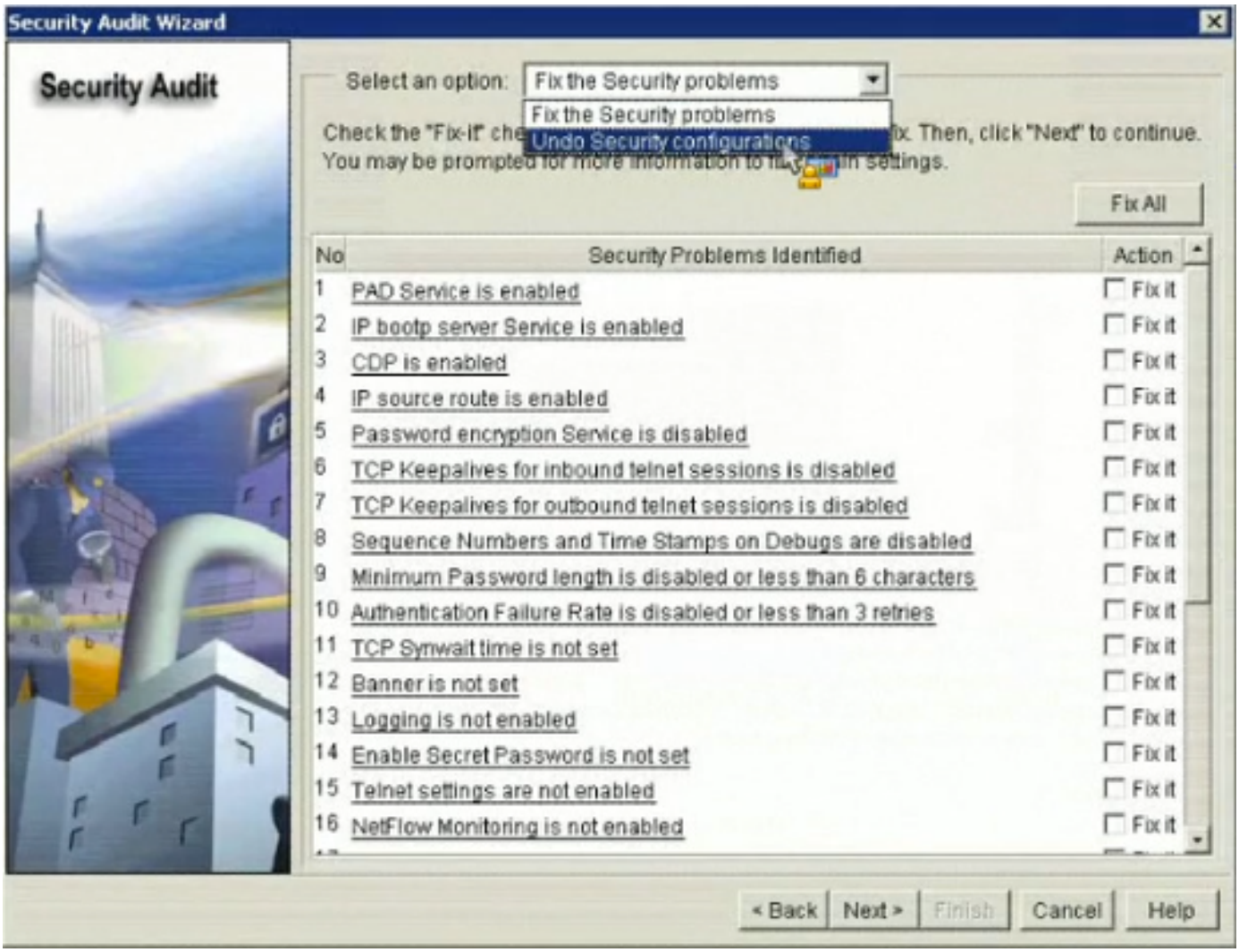




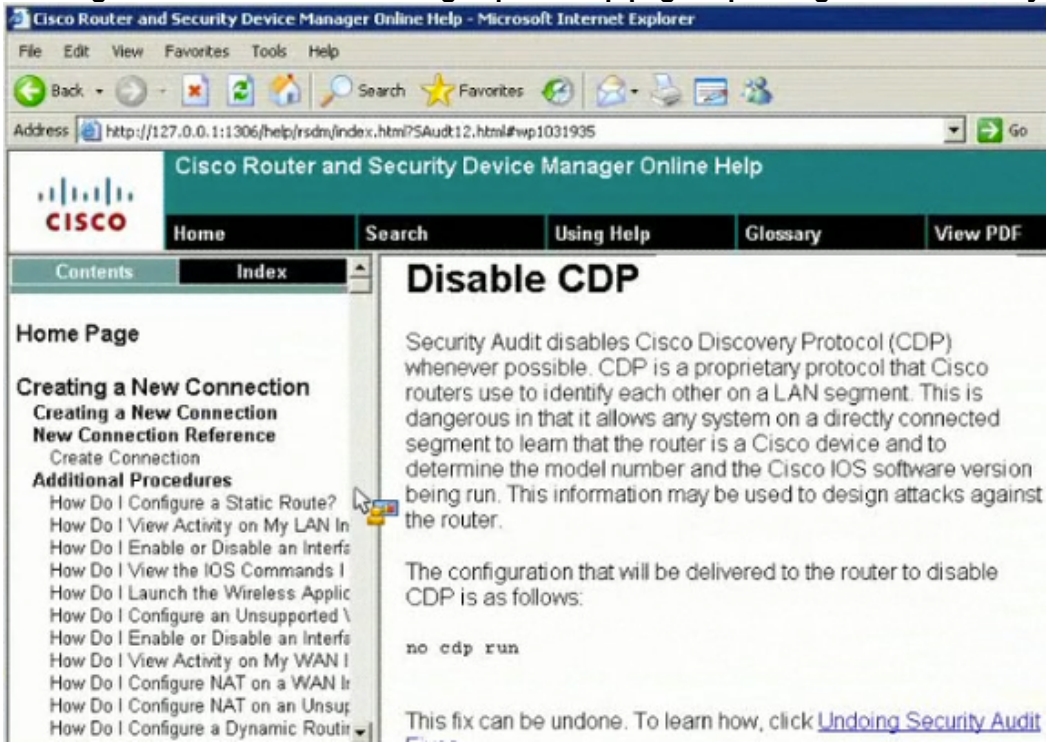
Note inside (trusted) and outside(untrusted) need to be designated:

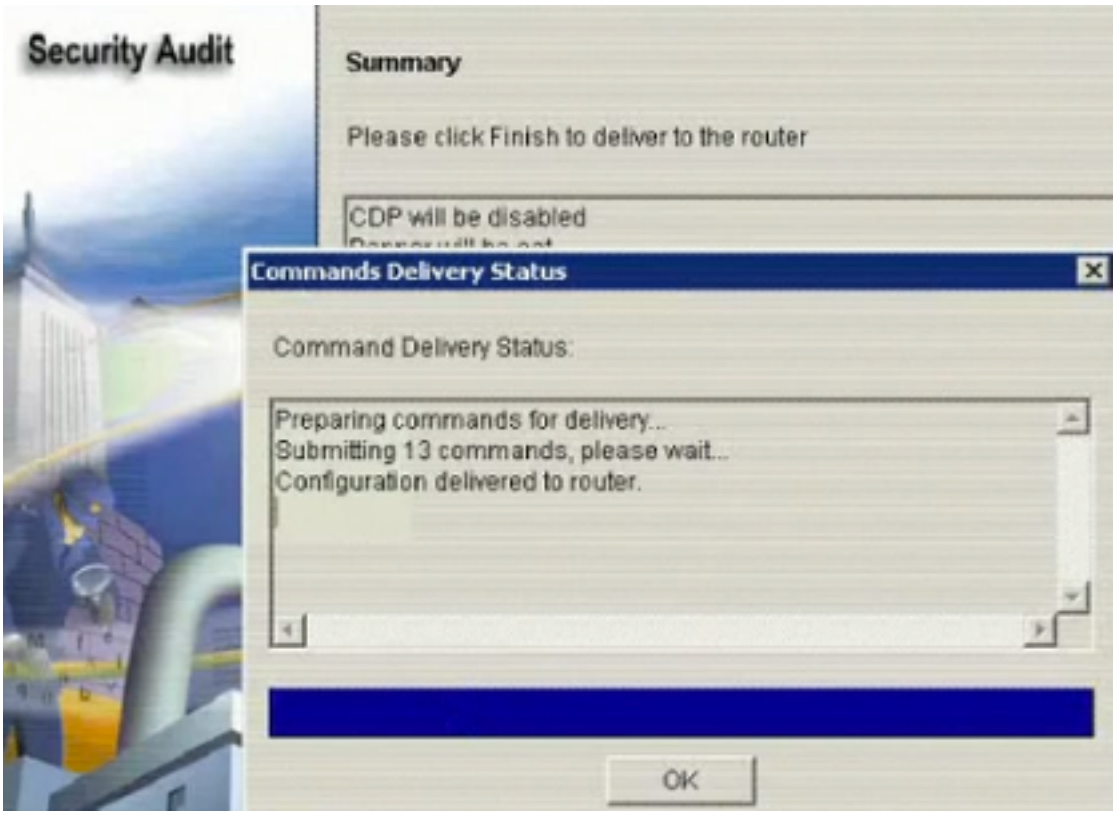

Tasks
Security Audit
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Additional Tasks
Security Audit Wizard
Security Audit
Security audit interface configuration
Select inside (trusted) and outside (untrusted) interfaces. You can select one or more inside (trusted)/outside (untrusted) interfaces.
Interface
Outside (Unt
Inside (Trust
FastEthernet0/0
FastEthernet0/1
Click next to perform the checking of security configurations on the router whether it is configured or not.
< Back
Next >
Finish
Cancel
Help
One-step lockdown
Security Audit
Internet


Security Audit Wizard
Security
Security Audit
Please wait while Security Audit checks if the recommended security settings are configured on the router.
No
Item Name
Status
24 Enable Telnet settings Not Passed
25 Enable NetFlow Monitoring Not Passed
26 Disable IP Redirects Not Passed
27 Disable IP Proxy Arp Not Passed
28 Disable IP Directed Broadcast Passed
29 Disable MOP service Not Passed
30 Disable IP Unreachables Not Passed
31 Disable IP Mask Reply Passed
32 Disable IP Unreachables on Null interface Not Passed
33 Enable Unicast RPF on all outside interfaces Not Passed
34 Enable Firewall on all outside interfaces Not Passed
35 Set Access class on HTTP server service Not Passed
36 Set Access class on VTY lines Not Passed
37 Enable SSH for access to the router Not Passed
38 Enable AAA Not Passed
Click "Close" to continue fixing the identified security problems or undoing the configured security configurations in the router.
Close
Save Report
< Back
Next >
Finish
Cancel
Help



If you chose One-Step Lockdown, it would automatically make all of these changes without asking (bad)
Clicking on the text of an item brings up the help page explaining the vulnerability or issue:





When applying the changes you selected, the commands are not dumped to the screen. You have to log into the IOS to see where the changes were made

```
!
interface FastEthernet0/0
 description $FW_INSIDE$
 ip address 10.0.0.6 255.255.255.0
 no ip redirects
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description $FW_OUTSIDE$
 ip address 200.0.16.6 255.255.255.0
 no ip redirects
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 no ip redirects
 encapsulation frame-relay IETF
 shutdown
 frame-relay lmi-type cisco
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 200.0.16.1
ip http server
 --More--
```

These are needed (cut off in graphic) to get SDM accessible in the web browser:
ip http server
ip http authentication local
no ip http secure-server

Video 6
IOS "Resilient configuration"
Protect IOS image and config file from accidental or malicious deletion
Move IOS image to a hidden file on disk that won't list with dir command
Copies running config to a hidden archive on disk
secure boot-image
secure boot-config
verify with show secure bootset - will reveal the hidden stuff

AAA stuff
TACACS+ Terminal Access Control Access Control System
- Cisco proprietary TCP port 49
- Cisco Access Control Server (ACS)
- Everything encrypted

RADIUS Remote Authentication Dial In User Service
- Open standard - UDP (!) 1645/1646 legacy ports, 1812/1813 standard ports
- Relies on upper layers to handle retransmission since it is UDP
- First port (like 1812) is for Auth and Auth, and the second is for Accounting
- Only key encrypted, the rest is plain-text

Only TACACS+ supports all of the IOS items, so would need it between routers, Catalyst switches ASA, PIX etc.
- (specifically noted was per-command authorization)

RADIUS mainly used for managing users; 802.1x auth, VPN user management database
Cisco Secure ACS supports both protocols and can run both simultaneously

Start the AAA process
- `aaa new-model`

Define authentication type and methods
- `aaa authentication login {default | list-name} {passwd-expiry method1 [method2...]}`
- `aaa authentication enable default method1 [method2...]`

Multiple methods allow for redundancy
- Last resort method should fall back to *local* in case AAA server is down

Apply list to desired line
- `Router(config)#line vty 0 4`
- `Router(config-line)#login authentication LIST1`

Lines without explicit list fall back to *default* method

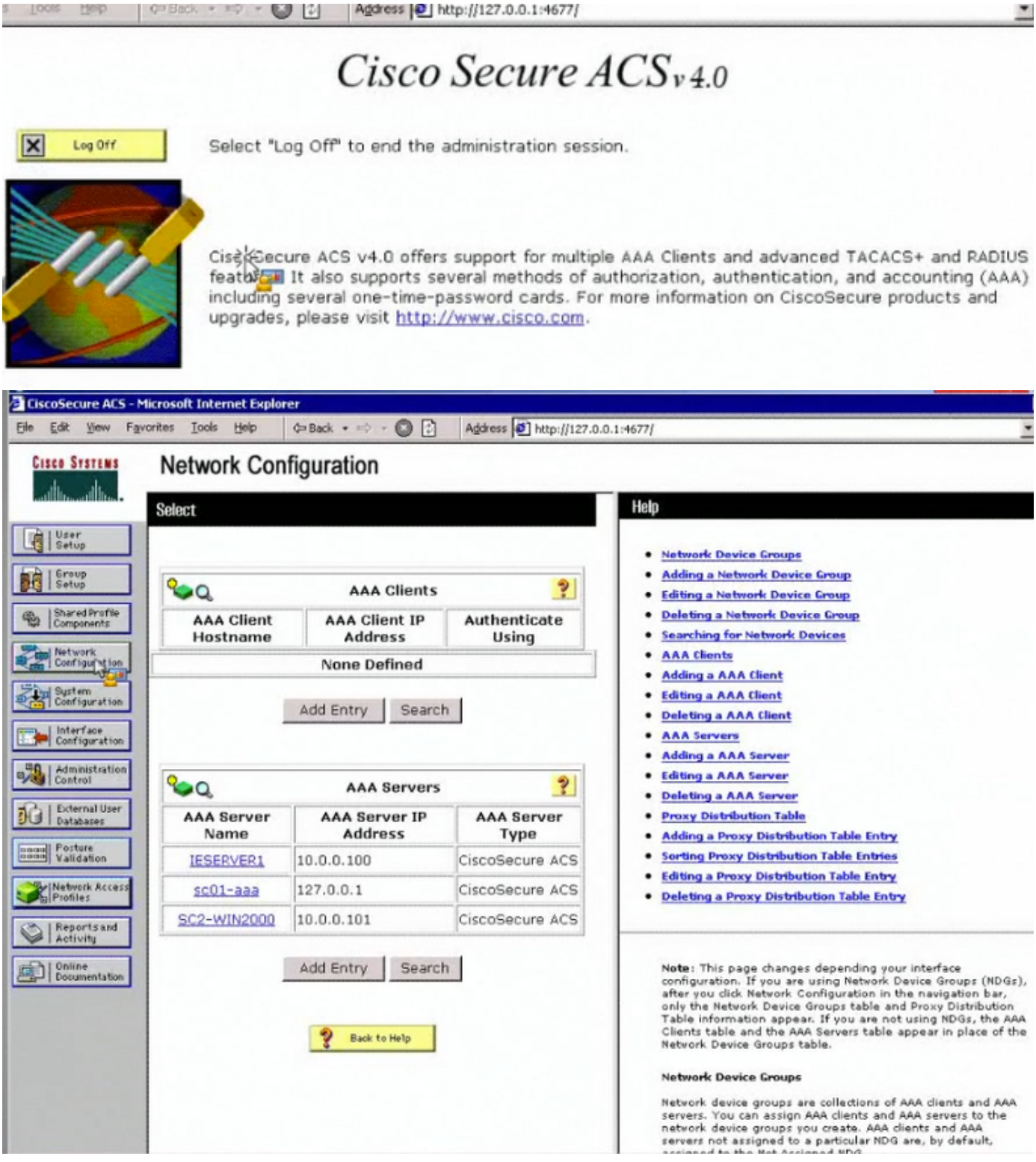
different list types to different lines
line types can have their own authentication types for example:
console authenticate locally
aux to RADIUS,
vty lines to TACACS+

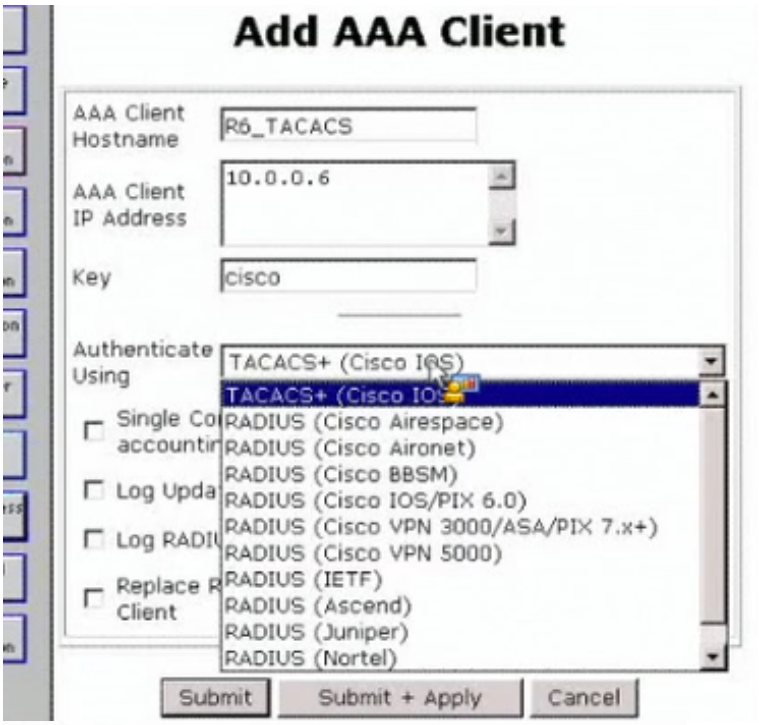
Login authentication and enable authentication, also PPP authentication (legacy)
default sets the default- login default none would apply to all tty, aux, console
Multiple methods is also an option in case one goes down for redundancy, eventually falling back to local

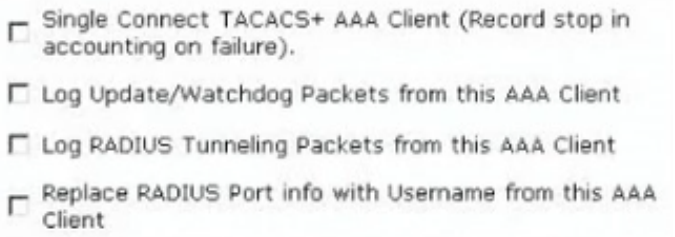
aaa new-model
tacacs-server host 10.0.0.100
tacacs-server key cisco2
radius-server host 10.0.0.100
radius-server key cisco2
aaa authentication login VTYLIST group tacacs local

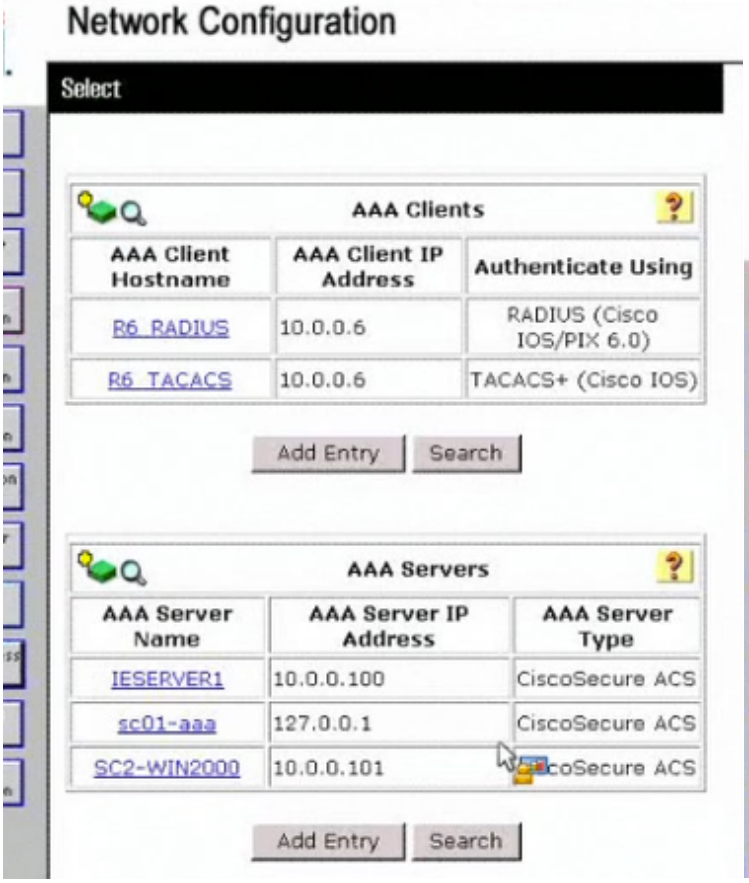
```
R6(config)#aaa new-model
R6(config)#radius-server host 10.0.0.100
R6(config)#radius-server key cisco
R6(config)#aaa authentication ?
  arap              Set authentication lists for arap.
  attempts          Set the maximum number of authentication attempts
  banner            Message to use when starting login/authentication.
  dot1x             Set authentication lists for IEEE 802.1x.
  enable            Set authentication list for enable.
  eou               Set authentication lists for EAPoUDP
  fail-message      Message to use for failed login/authentication.
  login             Set authentication lists for logins.
  password-prompt   Text to use when prompting for a password
  ppp               Set authentication lists for ppp.
  sgbp              Set authentication lists for sgbp.
  username-prompt   Text to use when prompting for a username
R6(config)#aaa authentication login ?
  WORD      Named authentication list (max 31 characters, longer will be
            rejected).
  default   The default authentication list.
R6(config)#aaa authentication login VTYLIST ?
  enable          Use enable password for authentication.
  group           Use Server-group
  krb5            Use Kerberos 5 authentication.
  krb5-telnet     Allow logins only if already authenticated via Kerberos V
                  Telnet.
  line            Use line password for authentication.
  local           Use local username authentication.
  local-case      Use case-sensitive local username authentication.
  none            NO authentication.
  passwd-expiry   enable the login list to provide password aging support
R6(config)#aaa authentication login VTYLIST group ?
  WORD      Server-group name
  radius    Use list of all Radius hosts.
  tacacs+   Use list of all Tacacs+ hosts.
R6(config)#aaa authentication login VTYLIST group tacacs ?
  enable       Use enable password for authentication.
  group        Use Server-group
  krb5         Use Kerberos 5 authentication.
  line         Use line password for authentication.
  local        Use local username authentication.
  local-case   Use case-sensitive local username authentication.
  none         NO authentication.
  <cr>
```

ekjhekhjfek


Address http://127.0.0.1:4677/
Cisco Secure ACS v4.0
Log Off
Select "Log Off" to end the administration session.
It also supports several methods of authorization, authentication, and accounting (AAA) including several one-time-password cards. For more information on CiscoSecure products and upgrades, please visit http://www.cisco.com.
CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address http://127.0.0.1:4677/
Cisco Systems
Network Configuration
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Select
AAA Clients
AAA Client Hostname
AAA Client IP Address
Authenticate Using
None Defined
Add Entry
Search
AAA Servers
AAA Server Name
AAA Server IP Address
AAA Server Type
IESERVER1
10.0.0.100
CiscoSecure ACS
sc01-aaa
127.0.0.1
CiscoSecure ACS
SC2-WIN2000
10.0.0.101
CiscoSecure ACS
Add Entry
Search
Back to Help
Help
Network Device Groups
Adding a Network Device Group
Editing a Network Device Group
Deleting a Network Device Group
Searching for Network Devices
AAA Clients
Adding a AAA Client
Editing a AAA Client
Deleting a AAA Client
AAA Servers
Adding a AAA Server
Editing a AAA Server
Deleting a AAA Server
Proxy Distribution Table
Adding a Proxy Distribution Table Entry
Sorting Proxy Distribution Table Entries
Editing a Proxy Distribution Table Entry
Deleting a Proxy Distribution Table Entry
Note: This page changes depending your interface configuration. If you are using Network Device Groups (NDGs), after you click Network Configuration in the navigation bar, only the Network Device Groups table and Proxy Distribution Table information appear. If you are not using NDGs, the AAA Clients table and the AAA Servers table appear in place of the Network Device Groups table.
Network Device Groups
Network device groups are collections of AAA clients and AAA servers. You can assign AAA clients and AAA servers to the network device groups you create. AAA clients and AAA servers not assigned to a particular NDG are, by default,


Add AAA Client
AAA Client Hostname
R6_TACACS
AAA Client IP Address
10.0.0.6
Key
cisco
Authenticate Using
TACACS+ (Cisco IOS)
RADIUS (Cisco Airespace)
RADIUS (Cisco Aironet)
RADIUS (Cisco BBSM)
RADIUS (Cisco IOS/PIX 6.0)
RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)
RADIUS (Cisco VPN 5000)
RADIUS (IETF)
RADIUS (Ascend)
RADIUS (Juniper)
RADIUS (Nortel)
Submit
Submit + Apply
Cancel


Single Connect TACACS+ AAA Client (Record stop in accounting on failure).
Log Update/Watchdog Packets from this AAA Client
Log RADIUS Tunneling Packets from this AAA Client
Replace RADIUS Port info with Username from this AAA Client


Network Configuration
Select
AAA Clients
AAA Client Hostname
AAA Client IP Address
Authenticate Using
R6_RADIUS
10.0.0.6
RADIUS (Cisco IOS/PIX 6.0)
R6_TACACS
10.0.0.6
TACACS+ (Cisco IOS)
Add Entry
Search
AAA Servers
AAA Server Name
AAA Server IP Address
AAA Server Type
IESERVER1
10.0.0.100
CiscoSecure ACS
sc01-aaa
127.0.0.1
CiscoSecure ACS
SC2-WIN2000
10.0.0.101
CiscoSecure ACS
Add Entry
Search


Reports and Activity
Select
Reports
TACACS+ Accounting
TACACS+ Administration
RADIUS Accounting
VoIP Accounting
Passed Authentications
Failed Attempts
Logged-in Users
Disabled Accounts
ACS Backup And Restore
Administration Audit
User Password Changes
ACS Service Monitoring