Basic Network Security

(Module 16)

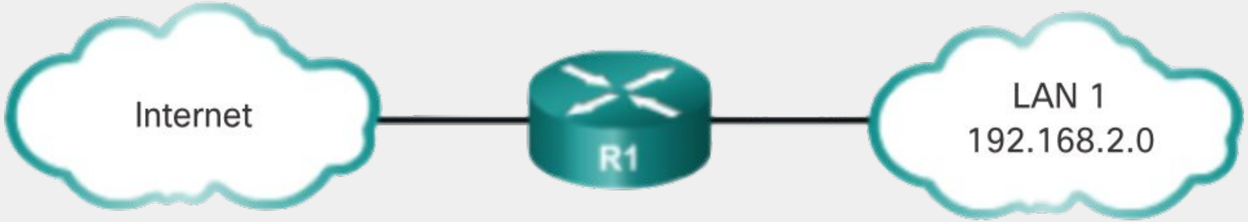
Security Terminology

- Edge router: router between the internal and external network
- ASA (Adaptive Security Appliance): special type of router used solely as a firewall
- DMZ (Demilitarized Zone): portion of a network not contained in a firewall
- View: set of commands available to a user
- IOS image: Cisco’s operating system for most devices
- Trap: automated informational message

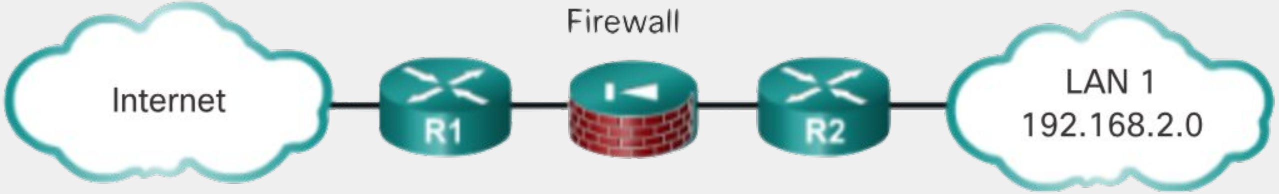
Approaches to Security

- Single-router approach
  - Best for small networks
  - Uses security features built into a standard router
- Defense-in-depth approach
  - More secure than a single router
  - Multi-layered: the edge router, the firewall, and an internal router that connects to the LAN
- DMZ approach
  - Similar to the defense-in-depth approach
  - Used when a server is hosted on the network
  - The DMZ can be a port on a router or a separate device

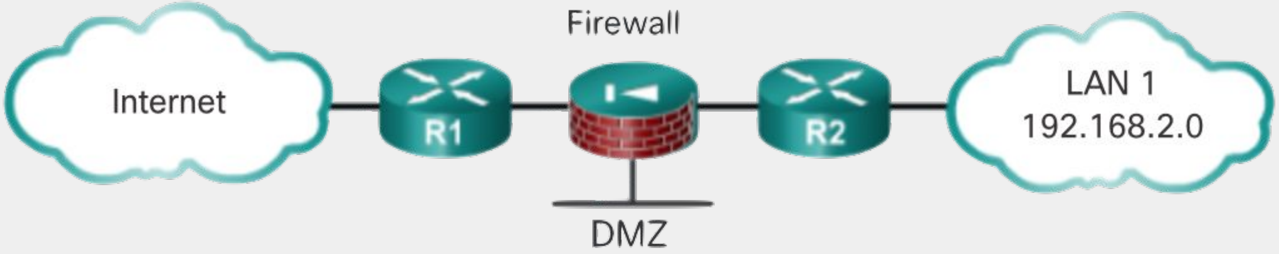
Single Router



Defense In-Depth



DMZ



Areas of Security

- Physical
  - Place critical devices in a locked room
  - Provide protections from electrical interference and overheating
  - Provide a backup power source
- Operating System
  - Ensure the devices have enough processing power/RAM to avoid DDOS attacks
  - Update the operating system as needed and keep backups of configuration files
- Router Hardening
  - Only allow access for authorized personnel
  - Disable unused interfaces and unnecessary services

Secure Administrative Access, Part 1

- Restrict availability
- Log administrative events
- Limit login attempts
- Only authorize privileges as needed
- Present a legal notification (motd banner)
- Ensure confidentiality
- Use secure passwords (`security passwords min-length`)

Secure Administrative Access, Part 2

- End unattended connections `exec-timeout #`
- Encrypt passwords
- Configure device users
- Log Failed Logins `login on-failure log`

Defending Administrative Routers

- Prefer local access over remote access
- Encrypt traffic if accessed remotely
- Place administrative devices in a separate network
- Use specific ACLs to restrict access to administrative traffic
- Use secure password protocols when creating and implementing passwords

Privilege Levels

- Privilege levels define which users can access which commands using numbers 0-15
- Preconfigured levels
  - 0: only enable, disable, exit, help, logout
  - 1: can only view parts of the configuration
  - 15: full access
- Levels 2-14 can be customized
- Higher levels automatically allow lower levels’ commands
- When adding a command to a higher level, it is automatically disallowed in lower levels

Views

- More specific way to assign privilege levels
- Three types of views:
  - Root: Same access as level 15 user; however, only a root view user can configure views
  - CLI: Group of non-hierarchical allowed commands
  - Superview: Consists of 1+ views
- Commands can be in more than one view
- Commands are not inherited by other views
- A password is required to change views

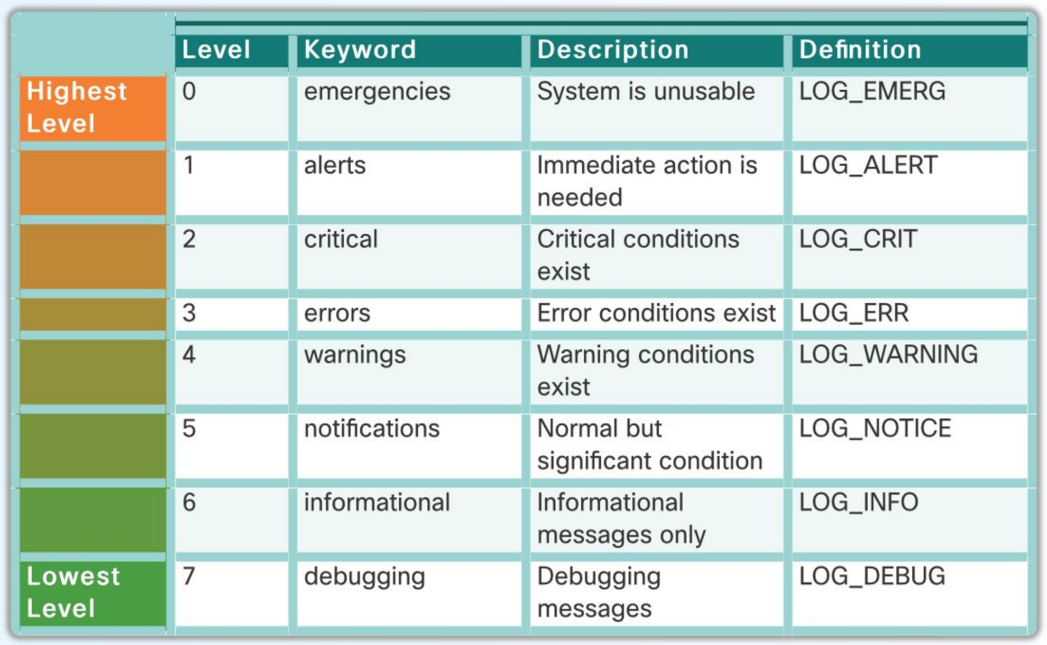
View Configuration

Step Description	Placement	Command	Category	Notes
enable AAA	router/switch config	aaa new-model	requirement	
create a view/enter view config	router/switch config	parser view [view name]	requirement	maximum of 15 views allowed must be in root view add "superview" to the end to create a superview
add a password	view config	secret [password]	requirement	
add a command to a view	view config	commands [parser mode] [include/include-exclusive /exclude] [optional: all] {[command]/interface [interface name]}	requirement	"parser mode" refers to which configuration mode a command is found (list of valid arguments: http://goo.gl/SlpGOu) "include-exclusive" includes a command and excludes it from any other views "all" includes all commands that start with a certain word example: “commands interface include all port-security”
enter a view	router/switch config	enable view [view name]	optional	leave out the view name to enter the root view
add a view to a superview	superview config	view [view name]	optional	
show all views	anywhere	do show parser view all	optional	

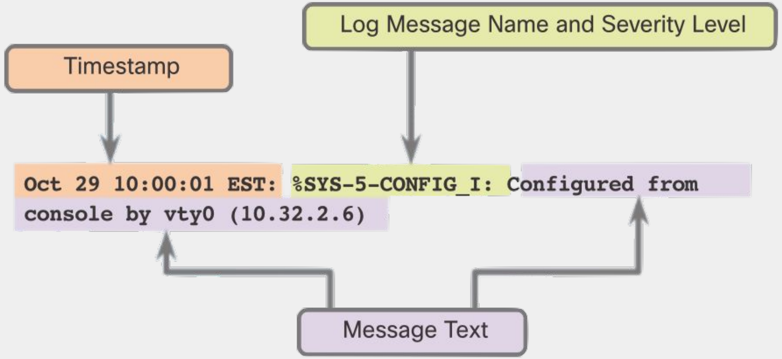
Syslog

- UDP protocol used to send log messages
- Logs ACL violations, login attempts, error messages, etc.
- Can be stored/sent in four ways:
  - Buffer: messages temporarily stored in RAM
  - Console: messages for a console line user
  - Terminal: messages for a remote line user
  - Syslog server: long-term storage on an end device

Syslog Messages



	Level	Keyword	Description	Definition
Highest Level	0	emergencies	System is unusable	LOG_EMERG
	1	alerts	Immediate action is needed	LOG_ALERT
	2	critical	Critical conditions exist	LOG_CRIT
	3	errors	Error conditions exist	LOG_ERR
	4	warnings	Warning conditions exist	LOG_WARNING
	5	notifications	Normal but significant condition	LOG_NOTICE
	6	informational	Informational messages only	LOG_INFO
Lowest Level	7	debugging	Debugging messages	LOG_DEBUG



Log Message Name and Severity Level

Timestamp

```
Oct 29 10:00:01 EST: %SYS-5-CONFIG_I: Configured from
console by vty0 (10.32.2.6)
```

Message Text

Syslog Configuration

Step Description	Placement	Command	Category
enable logging	any network device config	logging on	requirement
only log events at a certain security level	any network device config	logging trap [level]	optional
store log messages on a server	any network device config	logging host [server ip/hostname]	optional
send log messages from a specific interface	any network device config	logging source-interface [int type][int]	optional

SNMP (Simple Network Management Protocol)

- Application layer protocol
- Consists of three elements:
  - Manager: collects info from managed devices
  - Agents: send system info to the manager
  - MIB (Management Information Database): stores SNMP messages
- Creates security flaws
- Disable with “no snmp-server” command

NTP (Network Time Protocol)

- Used to synchronize time stamps across devices
- Uses strata to determine how far away (how many hops) the device is from a reliable timekeeping source
- Sends out periodic requests to the server to stay synchronized (can be configured to receive broadcasts instead)
- Publically available servers are typically used as opposed to configuring a server on a router

NTP Configuration

Step Description	Placement	Command	Category	Notes
add an NTP server	router/switch config	ntp server [server ip]	requirement	also enables NTP
update the hardware clock	router/switch config	ntp update-calendar	optional	
set a router as an NTP server for the network	router config	ntp master [stratum]	optional	stratum refers to the number of hops away from a reliable timekeeping source
configure the device to rely on broadcast messages	router/switch config	ntp broadcast client	optional	
create authentication keys	router/switch config	ntp authentication-key [key #] md5 [key value]	optional	required for authentication
select keys to use	router/switch config	ntp trusted-key [key #]	optional	required for authentication
enable authentication	router/switch config	ntp authenticate	optional	required for authentication disabled by default

Auto-Secure

- Script that makes recommendations on how to improve security
- Should only be used when first setting up a device
- More specific configurations should be applied after for stronger security
- Launch script using “auto secure” command

The “Login” Command

- “Login block-for” command must be used before other “login” commands can be entered
- When using this command, quiet mode will be triggered after a specified number of unsuccessful login attempts
- Quiet mode means that no remote login attempts can be made unless sent from a device allowed in the ACL

Command	Description	Placement	Notes
login block-for [seconds] attempts [# of tries] within [seconds]	blocks login attempts after incorrect passwords are entered within a certain time period	router config	
login [on-failure/on-success] log	logs failed/successful logins	router config	“every [# of attempts]” can be ended to the end of the command to specify how often a log message is created
login delay [seconds]	configures time required before another login attempt after an unsuccessful one	router config	
login quiet-mode access-class [ACL name/number]	enables quiet mode	router config	

General Security Commands

Command	Description	Placement	Notes
banner motd [delimiter] [message]	sets entrance message	any network device config	
enable secret [password]	sets an encrypted password for enable mode	any network device config	"level [level #] can be added before the password to restrict enable mode to a certain privilege level
exec-timeout [minutes] [optional: seconds]	sets logout timeout	con/aux/line config	
logging on	enables logging	any network device config	
privilege [mode] [command]	sets a privilege mode/level for a command	router/switch config	"mode" refers to exec/user/global/etc user modes adding "level [0-15]" before the command sets an associated level adding "all" before the level/command applies the privilege setting to all subcommands adding "reset" before the command resets the privilege levels"

General Security Commands (cont.)

Command	Description	Placement	Notes
security passwords min-length [0-16]	sets a minimum password length	router config	
service password-encryption	turns on password encryption	any network device config	
service timestamps log datetime msec	timestamps log messages	router/switch config	
username [username] password/secret [password]	adds a user to the local database	router/switch config	add "privilege [privilege level #] after the username to configure a privilege level
secure boot-config	secures config file	router config	
secure boot-image	secures router image	router config	can only be disabled through console mode
auto secure	starts auto secure script	any network device config	
no snmp-server	disables SNMP	router/switch config	

SSH Configuration

Step Description	Placement	Command	Category	Notes
assign a hostname	router config	hostname [hostname]	requirement	hostname cannot be default
assign a domain name	router config	ip domain-name [domain name]	requirement	
generate RSA keys and enable SSH	router config	crypto key generate rsa	requirement	"crypto key zeroize rsa" to reverse the command; will be prompted to enter key size from 360-4096 after entering the command (1024+ recommended)
create at least one user account	router config	username [username] secret [password]	requirement	"privilege [0-15]" can be added after the username to set a privilege level username is case-sensitive
only allow SSH	all vty lines	transport input ssh	requirement	
require local authentication	all vty lines	login local	requirement	
turn on management VLAN	management VLAN	no shutdown	requirement	management VLAN must have an IP
set an enable password	router config	enable [password/secret] [password]	requirement	
set an SSH version	router config	ip ssh version [1/2]	optional	default supports versions 1 and 2 (aka version 1.99)
set a timeout for inactive connections	router config	ip ssh time-out [0-120]	optional	time is in seconds
set a limit for authentication retries	router config	ip ssh authentication [# of retries]	optional	
test the SSH connection	command prompt of other device	ssh -l [username] [ip address]	optional	

Packet Tracer Lab

CCNA 2.5.1.2

Credits

Special thanks to all the people who made and released these awesome resources for free:

- Presentation template by SlidesCarnival
- Photographs by Unsplash