

CCNA Security

Chapter Two Securing Network Devices

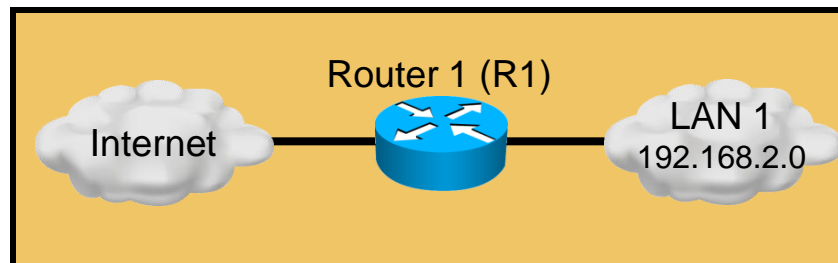
The Edge Router

- What is the edge router?
 - The last router between the internal network and an untrusted network such as the Internet
 - Functions as the first and last line of defense
 - Implements security actions based on the organization's security policies
- How can the edge router be secured?
 - Use various perimeter router implementations
 - Consider physical security, operating system security, and router hardening
 - Secure administrative access
 - Local versus remote router access

Perimeter Implementations

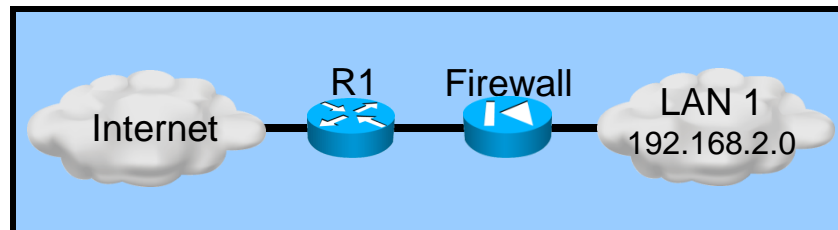
- **Single Router Approach**

A single router connects the internal LAN to the Internet. All security policies are configured on this device.



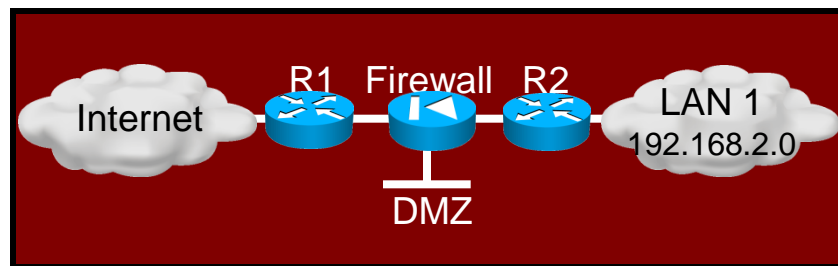
- **Defense-in-depth Approach**

Passes everything through to the firewall. A set of rules determines what traffic the router will allow or deny.



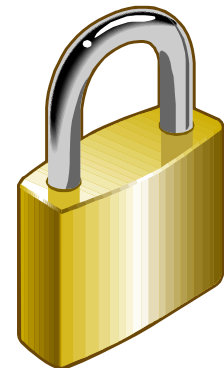
- **DMZ Approach**

The DMZ is set up between two routers. Most traffic filtering left to the firewall



Areas of Router Security

- Physical Security
 - Place router in a secured, locked room
 - Install an uninterruptible power supply
- Operating System Security
 - Use the latest stable version that meets network requirements
 - Keep a copy of the O/S and configuration file as a backup
- Router Hardening
 - Secure administrative control
 - Disable unused ports and interfaces
 - Disable unnecessary services



- Banners are disabled by default and must be explicitly enabled.

```
R1 (config) # banner {exec | incoming | login | motd | slip-ppp} d message d
```

- There are four valid tokens for use within the message section of the banner command:
 - **\$(hostname)**—Displays the hostname for the router
 - **\$(domain)**—Displays the domain name for the router
 - **\$(line)**—Displays the vty or tty (asynchronous) line number
 - **\$(line-desc)**—Displays the description that is attached to the line

- Configuring Router
- SSH Commands
- Connecting to Router

Complete the following prior to configuring routers for the SSH protocol:

1. Ensure that the target routers are running a Cisco IOS Release 12.1(1)T image or later to support SSH.
2. Ensure that each of the target routers has a unique hostname.
3. Ensure that each of the target routers is using the correct domain name of the network.
4. Ensure that the target routers are configured for local authentication, or for authentication, authorization, and accounting (AAA) services for username or password authentication, or both. This is mandatory for a router-to-router SSH connection.

Configuring the Router for SSH

```
R1# conf t
R1(config)# ip domain-name span.com
R1(config)# crypto key generate rsa general-keys
modulus 1024
The name for the keys will be: R1.span.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-
exportable...[OK]

R1(config)#
*Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has
been enabled
R1(config)# username Bob secret cisco
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
```

1. Configure the IP domain name of the network


2. Generate one way secret key

3. Verify or create a local database entry

4. Enable VTY inbound SSH sessions

Optional SSH Commands

```
R1# show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication
retries: 3
R1#
R1# conf t
Enter configuration commands, one per line.  End
with CNTL/Z.
R1(config)# ip ssh version 2
R1(config)# ip ssh time-out 60
R1(config)# ip ssh authentication-retries 2
R1(config)# ^Z
R1#
R1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 60 secs; Authentication
retries: 2
R1#
```

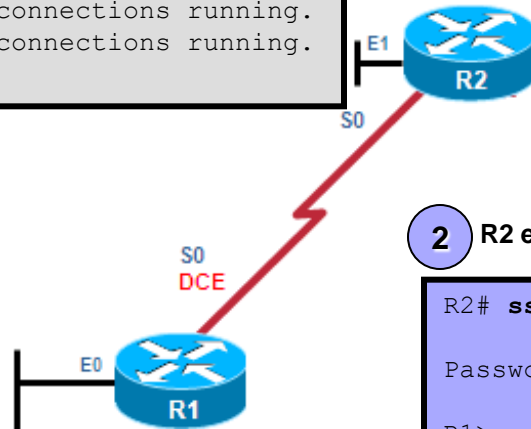


Connecting to the Router

There are two different ways to connect to an SSH-enabled router:

1 There are no current SSH sessions ongoing with R1.

```
R1# sho ssh
%No SSHv2 server connections running.
%No SSHv1 server connections running.
R1#
```



- Connect using an SSH-enabled Cisco router
- Connect using an SSH client running on a host.

2 R2 establishes an SSH connection with R1.

```
R2# ssh -l Bob 192.168.2.101
Password:
R1>
```

3 There is an incoming and outgoing SSHv2 session user Bob.

```
R1# sho ssh
Connection Version Mode Encryption Hmac State Username
0 2.0 IN aes128-cbc hmac-sha1 Session started Bob
0 2.0 OUT aes128-cbc hmac-sha1 Session started Bob
%No SSHv1 server connections running.
R1#
```

- Configuration Change Management
 - Know the state of critical network devices
 - Know when the last modifications occurred
 - Ensure the right people have access when new management methodologies are adopted
 - Know how to handle tools and devices no longer used
- Automated logging and reporting of information from identified devices to management hosts
- Available applications and protocols like SNMP

- When logging and managing information, the information flow between management hosts and the managed devices can take two paths:
 - **Out-of-band (OOB):** Information flows on a dedicated management network on which no production traffic resides.
 - **In-band:** Information flows across an enterprise production network, the Internet, or both using regular data channels.

- OOB management appropriate for large enterprise networks
- In-band management recommended in smaller networks providing a more cost-effective security deployment
- Be aware of security vulnerabilities of using remote management tools with in-band management

- Implementing Router Logging
- Syslog
- Configuring System Logging

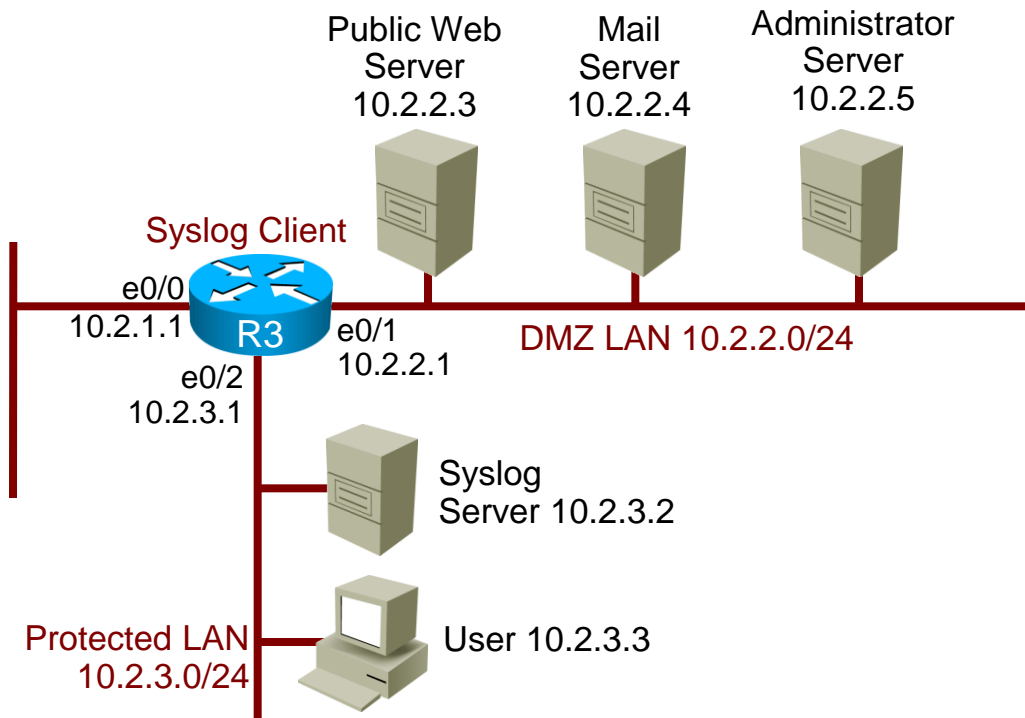
Configure the router to send log messages to:

- **Console:** Console logging is used when modifying or testing the router while it is connected to the console. Messages sent to the console are not stored by the router and, therefore, are not very valuable as security events.
- **Terminal lines:** Configure enabled EXEC sessions to receive log messages on any terminal lines. Similar to console logging, this type of logging is not stored by the router and, therefore, is only valuable to the user on that line.

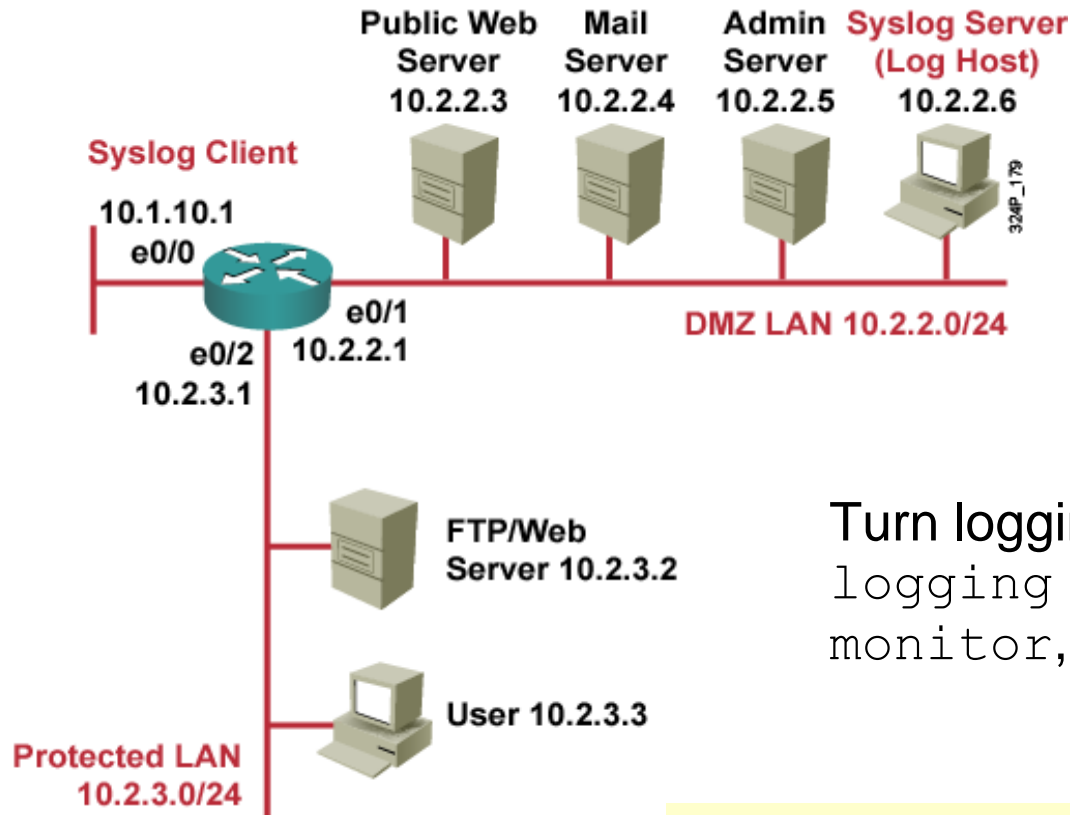
Implementing Router Logging

- Buffered logging: Store log messages in router memory. Log messages are stored for a time, but events are cleared whenever the router is rebooted.
- SNMP traps: Certain thresholds can be preconfigured. Events can be processed by the router and forwarded as SNMP traps to an external SNMP server. Requires the configuration and maintenance of an SNMP system.
- Syslog: Configure routers to forward log messages to an external syslog service. This service can reside on any number of servers, including Microsoft Windows and UNIX-based systems, or the Cisco Security MARS appliance.

- Syslog servers: Known as log hosts, these systems accept and process log messages from syslog clients.
- Syslog clients: Routers or other types of equipment that generate and forward log messages to syslog servers.



Configuring System Logging



Turn logging on and off using the logging buffered, logging monitor, and logging commands

1. Set the destination logging host

```
R3(config)# logging 10.2.2.6
```

2. Set the log severity (trap) level

```
R3(config)# logging trap informational
```

```
R3(config)# logging source-interface loopback 0
```

3. Set the source interface

```
R3(config)# logging on
```

4. Enable logging

- Clocks on hosts and network devices must be maintained and synchronized to ensure that log messages are synchronized with one another
- The date and time settings of the router can be set using one of two methods:
 - Manually edit the date and time
 - Configure Network Time Protocol



- Pulling the clock time from the Internet means that unsecured packets are allowed through the firewall
- Many NTP servers on the Internet do not require any authentication of peers
- Devices are given the IP address of NTP masters. In an NTP configured network, one or more routers are designated as the master clock keeper (known as an NTP Master) using the **ntp master** global configuration command.
- NTP clients either contact the master or listen for messages from the master to synchronize their clocks. To contact the server, use the **ntp server** *ntp-server-address* command.
- In a LAN environment, NTP can be configured to use IP broadcast messages instead, by using the **ntp broadcast client** command.

- There are two security mechanisms available:
 - An ACL-based restriction scheme
 - An encrypted authentication mechanism such as offered by NTP version 3 or higher
- Implement NTP version 3 or higher. Use the following commands on both NTP Master and the NTP client.
 - **ntp authenticate**
 - **ntp authentication *key md5 value***
 - **ntp trusted-key *key-value***

