

CISCO ACL Lab

TAL (ThinAirLabs), which has two sites, East and West, wants to connect to the internet. Each site has a Cisco Router, and plan to have a firewall in the future. They want to get online now and want you to configure the routers to filter inbound and outbound traffic.

TAL uses Services Plus, Inc. (SPI) for their internet access. SPI provides them with two systems:

Server1: 206.195.12.11 - Web, Mail, Telnet, FTP and DNS

Server2: 206.195.12.12 - Web, Secure Web, and FTP

The TAL network administrator has studied the IP traffic on the network. They have determined that:

- 40% Web based traffic (HTTP and SSL)
- 30% sending and retrieving email (SMTP and POP3)
- 15% nslookups using DNS
- 7% file transfers using active mode FTP
- 5% error and diagnostic messages using ICMP
- 3% other, such as Telnet

The security team, composed of managers, administrators, and users, is not sure why all of these protocols are needed, so they intended to implement a "deny all" policy.

Required Services

TAL needs to be able to send and retrieve email to SPI email servers.

TAL will allow all users to connect to any web site with normal and secure connections.

Anyone can FTP to SPI FTP sites. These sites only support active mode FTP.

PCE1 and PCW1 are FTP servers, and will allow active mode FTP from either site.

TAL users must be able to connect to the DNS server.

PCE2 and PCW2 only are allowed to telnet to SPI Server 1.

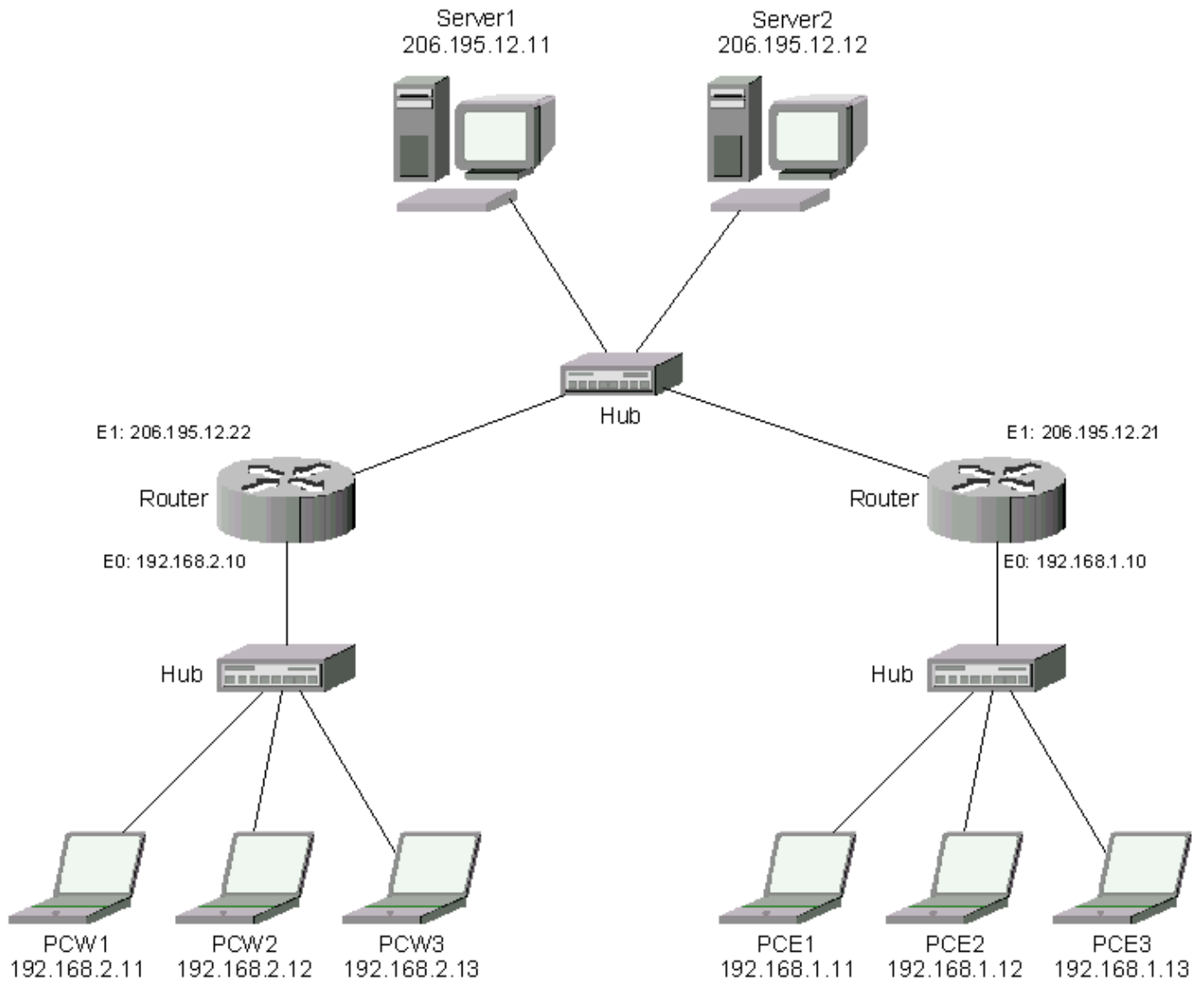
PCE2 and PCW2 only are allowed to telnet to their local routers (E0).

PCE3 and PCW3 are websites and are for internal site use only.

TAL allows all users to PING external sites.

No others services are allowed, inbound or outbound.

Lab Configuration



Checking the Configuration

Email Accounts (Configure Outlook Express):

The machine name is the userid and password on the mail system

example: PCW1: Email Name: pcw1 Password: pcw1

Each machine should be able to

- ping server1

- ping server2

- ping TAL local systems

- send / receive email

- access websites on server1 and server2

- FTP to server1, server2, PCW1, PCE1

Each system should NOT be able to

- ping TAL remote systems

- access other TAL remote site webserver (PCW3, PCE3)

ONLY PCE2 and PCW2

- Telnet to Server 1

- Telnet to Router

Only EAST

- Browse PCE1 website

Only WEST

- Browse PCW1 website