Testing ACLs

	Start Date	End Date
Network Build (Setup)		
Testing Date		

Table of Contents

Attendees

Name	Company	Position

Introduction

An introduction to the testing explaining briefly what the purpose of the test is, and what should be observed. Include a brief description of testing goals. List all tests you intend to run.

For example:

The purpose of this test plan is to add access control lists to the prototype network to secure unauthorized access to the server farm and to demonstrate that the access control lists are configured correctly. This revised prototype network is used to test various aspects of the proposed design.

- Test 1: Access Control Lists Test
  - Verify full connectivity from all PCs to all servers.
  - Plan access control lists to prevent unauthorized access to the server farm.
  - Configure access control lists on Distribution Layer devices and apply them to the proper interfaces in the proper direction.
  - Verify proper operation of the access control lists by verifying that permitted traffic gets through to the servers and unauthorized traffic is blocked.

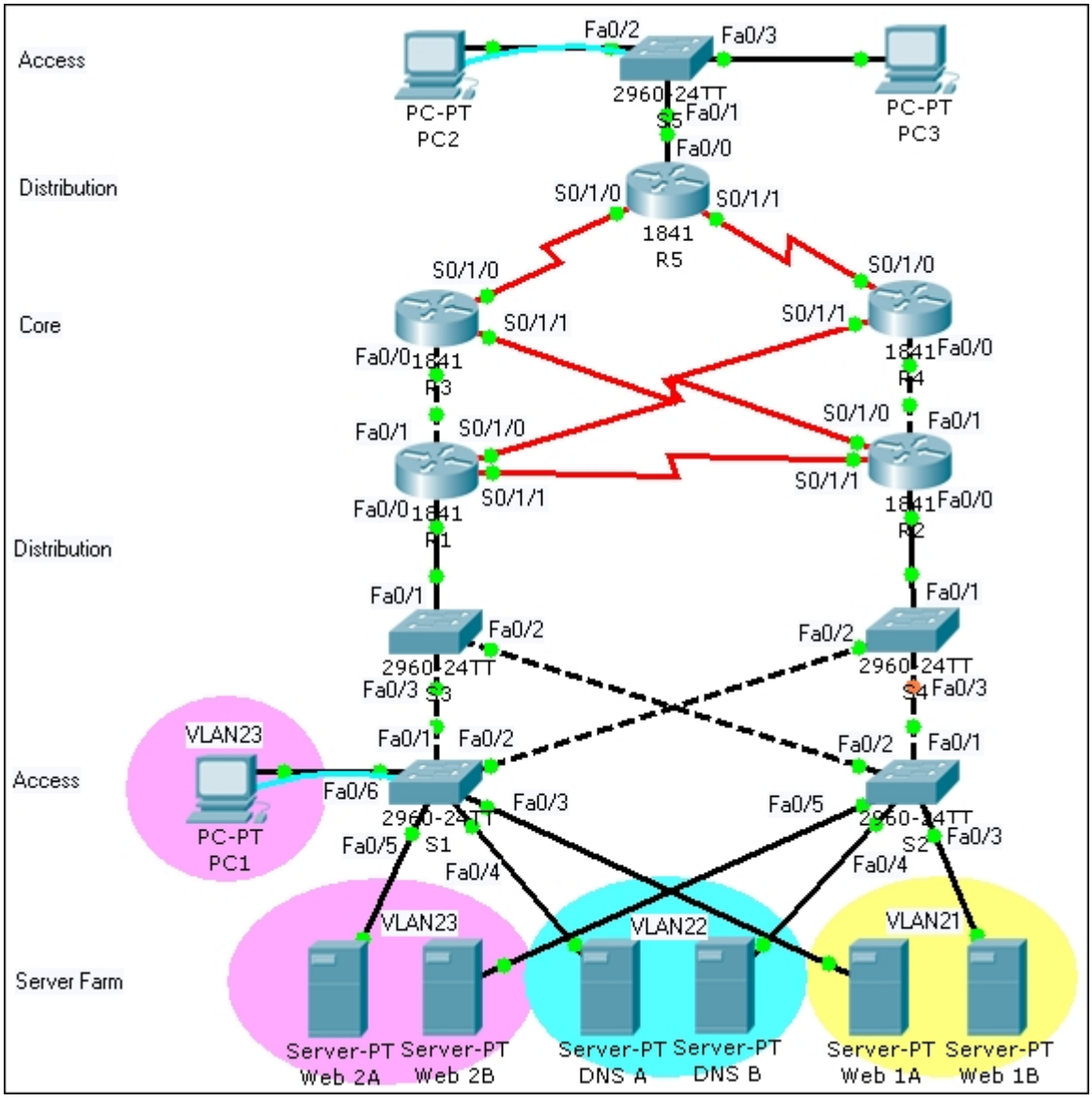
Equipment

List all of the equipment needed to perform the tests. Be sure to include cables, optional connectors or components, and software.

Qty. Req	Model	Any additional options or software required	Substitute	IOS Software Rev.
5	2960 Layer 2 switch	none	Any 2950 or 2960 model switch	12.2 or above
5	1841 ISR routers with 2 FastEthernet ports and 2 Serial ports	none	Any multilayer switch or router with minimum 2 FastEthernet ports and two serial port.	12.2 or above
3	Personal Computer end-devices	FastEthernet NIC	At least one PC and any other IP end-device (camera, printer, etc.)	Windows, MAC or Linux operating system.
6	Personal Computer Server	FastEthernet NIC	Any PC with web server and DNS software loaded	Windows, MAC, or Linux operating system
12	Cat 5 or above straight-through patch cables.	none	none	n/a
6	Cat 5 or above cross-over patch cables	none	none	n/a
5	V.35 DTE Serial Cables	None	None	n/a
5	V.35 DCE Serial Cables	None	None	n/a

Design and Topology Diagram

Place a copy of the prototype network topology in this section. This is the network as it should be built to be able to perform the required tests. If this topology duplicates a section of the actual network, include a reference topology showing the location within the existing or planned network. Initial configurations for each device must be included in the Appendix.



Device Designation	Interface	IP Address	Subnet mask	Gateway
R1	Fa0/0.1	172.18.2.1	255.255.255.0	N/A
R1	Fa0/0.21	172.18.21.1	255.255.255.0	N/A
R1	Fa0/0.22	172.18.22.1	255.255.255.0	N/A
R1	Fa0/0.23	172.18.23.1	255.255.255.0	N/A
R1	Fa0/1	172.18.0.17	255.255.255.252	N/A

R1	S0/1/0 * DTE	172.18.0.13	255.255.255.252	N/A
R1	S0/1/1 * DCE	172.18.0.25	255.255.255.252	N/A
R2	Fa0/0.1	172.18.2.2	255.255.255.0	N/A
R2	Fa0/0.21	172.18.21.2	255.255.255.0	N/A
R2	Fa0/0.22	172.18.22.2	255.255.255.0	N/A
R2	Fa0/0.23	172.18.23.2	255.255.255.0	N/A
R2	Fa0/1	172.18.0.21	255.255.255.252	N/A
R2	S0/1/0 * DTE	172.18.0.10	255.255.255.252	N/A
R2	S0/1/1 * DTE	172.18.0.26	255.255.255.252	N/A
R3	Fa0/0	172.18.0.18	255.255.255.252	N/A
R3	S0/1/0 * DTE	172.18.0.1	255.255.255.252	N/A
R3	S0/1/1 * DCE	172.18.0.9	255.255.255.252	N/A
R4	Fa0/0	172.18.0.22	255.255.255.252	N/A
R4	S0/1/0 * DTE	172.18.0.5	255.255.255.252	N/A
R4	S0/1/1 * DCE	172.18.0.14	255.255.255.252	N/A
R5	Fa0/0	172.18.1.1	255.255.255.0	N/A
R5	S0/1/0 * DCE	172.18.0.2	255.255.255.252	N/A
R5	S0/1/1 * DCE	172.18.0.6	255.255.255.252	N/A
S1	VLAN1	172.18.2.3	255.255.255.0	172.18.2.1
S2	VLAN1	172.18.2.4	255.255.255.0	172.18.2.1
S3	VLAN1	172.18.2.5	255.255.255.0	172.18.2.1
S4	VLAN1	172.18.2.6	255.255.255.0	172.18.2.1
S5	VLAN1	172.18.1.2	255.255.255.0	172.18.1.1
PC1		172.18.23.10	255.255.255.0	172.18.23.1
PC2		172.18.1.10	255.255.255.0	172.18.1.1
PC3		172.18.1.11	255.255.255.0	172.18.1.1
Web 1A		172.18.21.3	255.255.255.0	172.18.21.1
Web 1B		172.18.21.4	255.255.255.0	172.18.21.2
DNS A		172.18.22.3	255.255.255.0	172.18.22.1
DNS B		172.18.22.4	255.255.255.0	172.18.22.2
Web 2A		172.18.23.3	255.255.255.0	172.18.23.1
Web 2B		172.18.23.4	255.255.255.0	172.18.23.2

Figure 1: Topology - Prototype test topology.

Add a description about this design here that is essential to provide a better understanding of the testing or to emphasize any aspect of the test network to the reader.

For each test to be performed state the goals of the test, the data to record during the test, and the estimated time to perform the test.

Test 1. Description: Access Control Lists Test

Goals of Test:
The goal of the test is to verify that access control lists are properly configured and applied to permit authorized traffic and to block unauthorized traffic.

Data to Record:
Configurations Router configurations ACL information Ping Test Output Web page access information

Estimated Time:
120 minutes

Test 1. Procedures:

Itemize the procedures to follow to perform the test.

Step 1: Verify full connectivity from all PCs to all servers.

1. From PC1 and PC2 ping all of the servers in the topology. Record the results.
2. From PC1 and PC2 access the following web pages: www.web1a.com, www.web1b.com, www.web2a.com, and www.web2b.com. Record the results.
3. From PC2, ping the Fa0/1 interface of routers R1 and R2 to verify connectivity and then telnet to routers R1 and R2 and get the "**`show running-config`**" output. Copy and paste the results into a document for later use.

Step 2: Plan access control lists to prevent unauthorized access to the server farm.

1. Design an access control list numbered 101 to allow only web access from hosts on the internal network, 172.18.0.0/16, to any device and deny all other traffic. Design an access control list numbered 102 to allow only DNS access from hosts on the internal network, 172.18.0.0/16, to any

device and deny all other traffic.

Step 3: Configure and apply access control lists.

1. Telnet to routers R1 and R2 and add both access control lists and apply them on to the proper interfaces in the proper direction to protect the servers connected to that interface.

Step 4: Verify proper operation of the access control lists.

1. From PC1 and PC2 ping all of the servers in the topology. Record the results.
2. From PC1 and PC2 access the following web pages: www.web1a.com, www.web1b.com, www.web2a.com, and www.web2b.com. Record the results.
3. Telnet to routers R1 and R2 and document the final cofiguration using **"show running-config",** and **"show access-lists".**

Test 1. Expected Results and Success Criteria:

List all of the expected results. Specific criteria that must be met for the test to be considered a success should be listed. An example of specific criteria is: "A requirement that ping response times cannot exceed 100 ms."

1. Prior to configuring access control lists both PCs can ping all servers and access all web pages.
2. After configuring access control lists, PC2, representing a legitimate inside user, can not ping any server but can access all web pages.
3. After configuring access control lists, PC1, representing a PC set up to maintain switch configurations, can ping servers in its own VLAN, can not ping other servers, and can not access any web pages.

4. Test 1. Results and Conclusions

Record the results of the tests and the conclusions that can be drawn from the results.

Appendix

Record the starting configurations, any modifications, log file or command output, and any other relevant documentation.