

15 - Using Client Authentication

Objectives

- Know the daemons that Client Authentication uses
- Know the port numbers used by Client Authentication daemons
- Know the different sign-on methods for Client Authentication
- Use client authentication with FTP

Approximate time for completing each section

Section 1	Client Authentication	45 minutes
	Total time	45 Min

Prerequisites

- Complete Module 14
- Virtual machines MgmtSite1, fwsite1 & classrouter must be running

Contents

1	Client Authentication	3
1.1	Client Authentication Daemons & Process	3
1.1.1	Authentication Daemons & Supported Services	3
1.1.2	Client Authentication – Policy Global Properties	3
1.1.3	Welcome Message	3
1.1.4	Client Authentication and the Perimeter Router/Firewall	4
1.2	Client Authentication Details	4
1.2.1	Client Authentication – aclientd, Port 259	4
1.2.2	Client Authentication – ahclientd, Port 900	4
1.2.3	Controlling the Number of Sessions and Time Period	5
1.2.4	Client Authentication Sign On Methods	5
1.3	Authentication Using FTP – Manual Authentication	6
1.3.1	Add an Authentication rule	6
1.3.2	Installing the Policy and Testing FTP Access	6
1.4	Authentication Using Secure Shell	7
1.4.1	Add an Authentication rule	7
1.4.2	Installing the Policy and Testing Secure Shell Access	7
1.5	Authentication Using a Different Port Number	8
1.5.1	Edit the fwauthd.conf File	8
1.5.2	Test the Authentication Using a Different Port Number	9
1.5.3	Add a Rule to Allow Port 2590 Access to the Firewall	9
1.5.4	Port 259 and 900 Versus a Different Port	10