

9 - SmartView Monitor

Objectives

- Know the type of information monitored
- Know how to set alert types for specific events
- Know the licensing requirement for SmartView Monitor
- Use SmartTracker Active Log to block connections
- User SmartView Monitor to view blocked connections
- Use SmartView Monitor to block connections

Prerequisites

- Complete Module 8
- Virtual Machines MgmtSite1, fwsite1 & classrouter must be running

Approximate time for completing each section

Section 1	SmartView Monitor	10 minutes
Section 2	SmartView Monitor Traffic Statistics	20 minutes
Section 3	Suspicious Activity Monitoring (SAM)	20 minutes
	Total time	50 Min

Contents

1 SmartView Monitor.....	3
1.1 Gateway Status.....	3
1.1.1 Filtered views.....	3
1.1.2 Gateway Properties.....	3
1.1.3 Other Objects	3
1.2 SmartCenter Object	4
1.2.1 System Information.....	4
1.2.2 Licences.....	4
1.2.3 Certificate Authority	4
1.2.4 Policy State and Connected Clients.....	4
1.2.5 Disconnecting SmartConsole Clients.....	4
1.3 Firewall Object	5
1.3.1 System Information.....	5
1.3.2 Network Activity	5
1.3.3 Licenses.....	5
1.3.4 Security Servers	5
1.3.5 Advanced Information	6
1.4 Threshold Settings	6
1.4.1 Global, None, Custom	7
1.4.2 System Alert Daemon	7
2 SmartView Monitor Traffic Statistics	8
2.1 Traffic Statistics.....	8
2.1.1 Enable SmartMonitor on the Firewall.....	8
2.1.2 Generate Some Traffic	8
2.1.3 Traffic & System Counters	9
3 Suspicious Activity Monitoring (SAM).....	11
3.1 Suspicious Activity Monitoring and Filter Location	11
3.2 Using SmartView Tracker – Active Log	11
3.2.1 Create a Suspicious Connection.....	11
3.2.2 View Connection in the SmartView Tracker – Active Tab	11
3.2.3 Select Tools – Block Intruder	11
3.2.4 Kill Connection for three Minutes	11
3.2.5 Test Connection Rejects and Alerts.....	11
3.2.6 Clear all SAM Connections – ‘fw sam –f All –D’	12

3.2.7 Test Connections Work	12
3.3 Using SmartView Monitor - Tools	12
3.3.1 Create a Suspicious Connection.....	12
3.3.2 View Connection in the SmartView Tracker – Active Tab	12
3.3.3 Select Tools and Block Intruder	12
3.3.4 View all SAM rules in the SmartMonitor.....	12
3.3.5 Delete the SAM Rule.....	13
3.3.6 Create a New SAM Rule Within SmartMonitor	13
3.3.7 Test the New SAM Rule	13