FireTower Security Solution Evaluation Road Map

A Three-Step Process

Summary:
FireTower Security Software provides automatic, real-time protection against zero-day malware, and performs continuous monitoring with ongoing attack alerts and live forensics for incident response investigation.

The FireTower Service software can be hosted as an application on a Windows (desktop or server OS). Any Windows machine (Windows XP/sp3, Vista, 7,8,10 and Windows Server 2003R2, 2008R2, 2012R2, and 2016) can be protected through this FireTower Service using FireTower Client agent software. The FireTower Service PC can also be protected as an endpoint by installing FireTower Client software.

The PC to host FireTower Service requires a Windows x64 architecture with Microsoft PowerShell 3.0 and above. The preferred FireTower Service PC is a Windows 10 x64 machine (preinstalled with PowerShell is 5.0)

Installation and Deployment steps:

1. At your PC to host FireTower Service software
2. Click to download FireTower Server and Cyber Console Installer Software (Step 1 below)
3. If you have received a product activation key, please use that key to activate the FireTower Service during the installation process, otherwise use the product key in Step 1 below to activate your copy of FireTower Service.
4. During the FireTower Service Installation process, the most likely hiccup is the unavailability of TCP ports (80, 443, and 3306) needed by FireTower Service. Please refer to the Appendix 1 at the end of this document to resolve this issue and rerun FireTower Server and Cyber Console Installer Software
5. After FireTower Service is successfully installed, log in to WinCyCOn.exe (ID: admin, and default password: admin) and go to Account Management Tab, Create an enrollment, download the enrollment package and unzip the package. (Please make sure you unzip the package. DO NOT run FireTowerGuard_ENT.exe from the

zip file directly) (Please refer to the document: FireTower Quick Start Guide for Deployment and Operations)

6. Run FireTowerGuard_ENT.exe at the PC hosting FireTower Service, after installation is completed. Wait for FireTower Client software is initialized, this PC will be listed at the Dashboard of Cyber Console (WinCyCon.exe)
7. Repeat the above process on each and every Windows PC to be protected.
8. For FireTower Cyber Console operations please refer to the included FireTower Quick Start Guide for Deployment and Operations
9. Please refer to the Appendix 2 to configure FireTower client software at endpoint computers to access FireTower Service over internet

Preamble: FireTower Security Solution Overview

Step 1: Install FireTower Server software on a PC

Download FireTower Server and Cyber Console Installer Software

Use the following 30-day trial key to activate your FireTower Server license:
070BB-C2A07-2FAF5-16D68-A6F966

a. Does not have to be a dedicated PC to host FireTower Server software
b. For FireTower Server only, any Windows x64 system with Microsoft PowerShell version 3 or above. Preferred Windows 10 x64 system
c. Note: If communication ports 80 and/or 443 are occupied on the PC that you intend to install FireTower Server please consult this webpage to identify and resolve the conflict.

Step 2: Deploy FireTower client software to computers to be protected

a. FireTower Quick Start Guide for Deployment and Operations
b. Supported endpoint computers:
Windows XP-SP3/Vista/7/8.1/10/2003R2/2008R2/2012R2/2016
c. For Enterprise network, remote deployment is available for Active Directory Domain Systems.

Step 3: Perform Security Operations

a. Continuous Monitoring
b. Automated Detection and Containment at endpoint computers
c. Live Forensic Investigation
d. FireTower Quick Start Guide for Deployment and Operations
Slide 18-42

References:

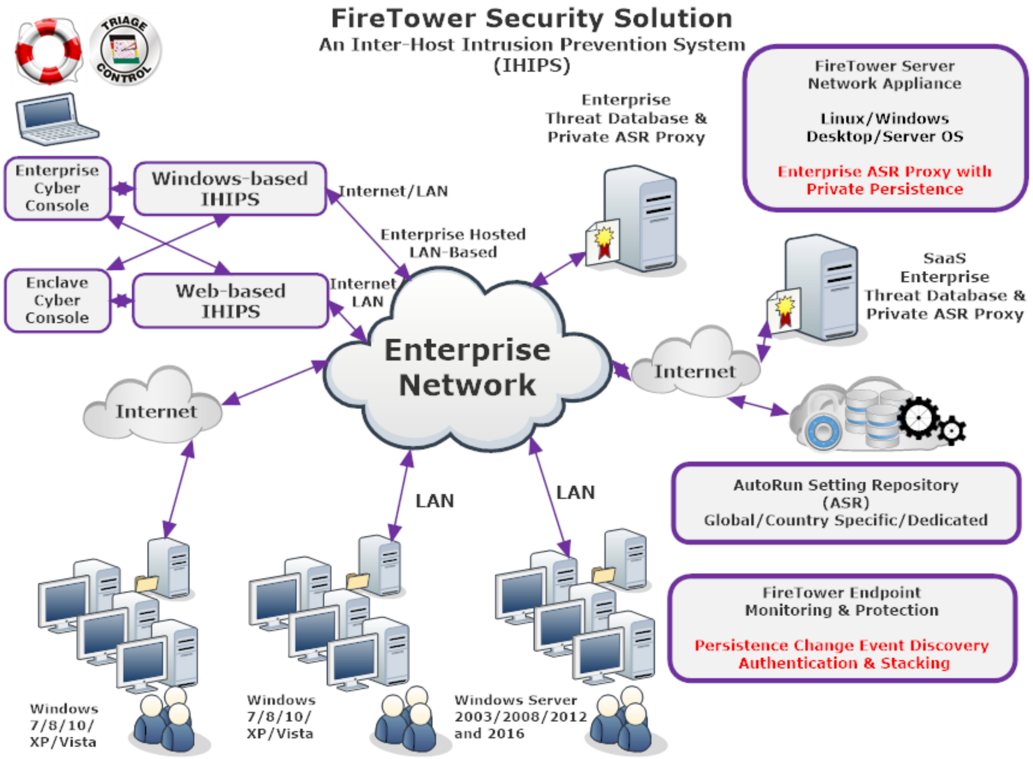
1. FireTower Security Solution Overview
2. FireTower Quick Start Guide for Deployment and Operations
3. FireTower Installation and Operation Troubleshooting Guide
4. FireTower Server Installation Software Resource Page
5. WebSites: SampanSecurity.com and FireTower.net
6. Contact Us

FireTower Security Solution Background Information

1. FireTower Overview

FireTower discovers and authenticates critical change events at endpoint computers and synthesizes discoveries to a centralized enterprise threat database maintained by the FireTower Server service. Through this threat database, FireTower provides an interactive threat exploration interface with built-in analytics to hunt for indicators of compromise, to deliver comprehensive endpoint visibility and to enhance the detection and containment of malicious activities.

2. FireTower Architecture and Components


FireTower Security Solution
An Inter-Host Intrusion Prevention System (IHIPS)
TRIAGE CONTROL
Enterprise Threat Database & Private ASR Proxy
FireTower Server Network Appliance
Linux/Windows Desktop/Server OS
Enterprise ASR Proxy with Private Persistence
Enterprise Cyber Console
Windows-based IHIPS
Internet/LAN
Enterprise Hosted LAN-Based
Enclave Cyber Console
Web-based IHIPS
Internet LAN
SaaS Enterprise Threat Database & Private ASR Proxy
Enterprise Network
Internet
Internet
AutoRun Setting Repository (ASR) Global/Country Specific/Dedicated
LAN
LAN
FireTower Endpoint Monitoring & Protection
Persistence Change Event Discovery Authentication & Stacking
Windows 7/8/10/ XP/Vista
Windows 7/8/10/ XP/Vista
Windows Server 2003/2008/2012 and 2016

3. FireTower Enterprise Security Tasks

1. Zero-day attack Detection and Containment

FireTower Client software to detect and contain incoming Zero-day malicious software in real-time based on the group specific security posture.

2. Continuous Monitoring for Security Operations Center

FireTower delivers the continuous monitoring capabilities using Cyber Console (CyCon) Dashboard for the enterprise security situational awareness and Inter-Host Intrusion Prevention System (IHIPS) Activity Tab for attack in progress detection.

3. **Incident Response and Forensic Investigation**

   FireTower delivers live forensic support by continuously monitoring persistence mechanism change events. Incident response can then be conducted instantly when a breach is suspected thus eliminating the delay and extra cost of using external professional investigators.

FireTower Security Solution Appendix 1:

Communication ports needed for FireTower Service Operations

FireTower Server requires the following TCP Communication Ports:

1. Port: 80 for HTTP (C:\xampp\apache\bin\httpd.exe
2. Port 443 for HTTPS (C:\xampp\apache\bin\httpd.exe
3. Port 3306 for MySQL (C:\xampp\mysql\bin\mysqld.exe

The FireTower Server Installer software will make sure these prerequisites are met, if not you could not proceed with the FireTower Server installation.

Please note the FireTower Server Installer software will prompt you with the current application names and Process IDs that occupy these ports, please free these ports first before re-run the FireTower Server Installer software.

If communication ports 80 and/or 443 are occupied on the PC that you intend to install FireTower Server please consult this webpage to identify and resolve the conflict.

Symptom: "FireTower Server Installer Prerequisite Not Met" when you try to run FireTower Server Installer.

Possible scenarios:

1. If you have VMware Workstation installed, (port 443 used)
2. If you are running from Windows 10 (port 80 used by IIS)
3. If you are running from Windows 7 SP1 (port 80 used by NT Kernel)
4. If you are running from Windows 7 SP1 (port 80 used by W3SVC or MSDepSvc, Web Deployment Agent Service)

FireTower Security Solution Appendix 2:

Accessing FireTower Server over internet

1. To enable endpoint PC protection or FireTower Cyber Console administration over internet, FireTower Server IP address has to be routable or with DNS registration
2. Windows Cyber Console, WinCyCon.exe (x86 or x64) can be copied to any PC to access FireTower Server over internet or intranet.
3. FireTower Server PC: modify FireTower Server PC IP address with a different IP address or domain name:
    a. Edit C:\xampp\cycon\config\cycon.ini file
    b. Remove the ";" in front of the line "server_name"
    c. Enter new FireTower Server PC IP address or domain name and save the cycon.ini, and reboot FireTower Server PC
4. FireTower Client PC for protection over internet
    a. Edit server_name key value field of registry key: HKEY_LOCAL_MACHINE:\software\Sampan Security\FireTower at endpoint computer with a routable FireTower Server PC IP address or domain name
    b. Reboot endpoint computer