Snort:

- SNORT is network-based Intrusion Detection System written in C programming.
- SNORT was developed in 1998 by Martin Roesch and now it is developed by Cisco.
- Snort is a free open source network intrusion detection system (IDS) and (IPS).
- Free open source software can also be used as packet sniffer to monitor the system.
- Network admin can use it to watch all the incoming packets & find dangerous one.
- Snort Features, Real-time traffic monitor, Packet logging and Analysis of protocol.
- Content matching, OS fingerprinting & can be installed in any network environment.

Sourcefire:

- Sourcefire was technology company developed network security hardware & software.
- The Sourcefire was founded in 2001 by Martin Roesch, the creator of Snort IPS and IDS.
- The Sourcefire company was acquired by Cisco company for $2.7 billion in July 2013.
- At that time, the Sourcefire was one of the top leaders in the cybersecurity industry.
- For its intrusion detection system (IDS), intrusion prevention system & NGFW solutions.
- Company created a commercial version of the Snort software, the Sourcefire 3D System.
- Which evolved into the company's Firepower line of network security products etc.
- After that Cisco has pull the Sourcefire technologies on various existing Cisco appliances.
- Such as, Adaptive Security Appliance 5500-X series and Integrated Services Router (ISR).
- Later, Cisco has released new hardware platforms, such as Firepower 2100 Series & 4100.
- All these new hardware platforms were also implement the Sourcefire technologies.

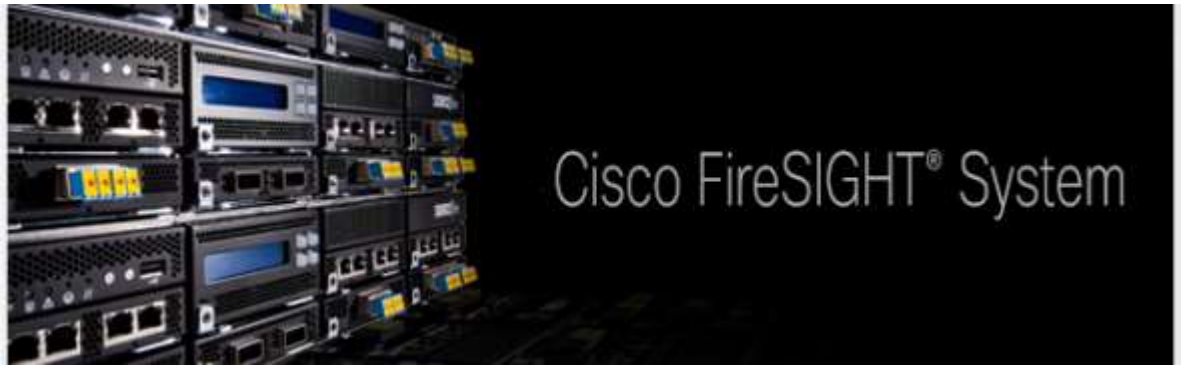
SOURCEfire®

Software Version	Management Appliance
Version 4.x	Defense Center (DC)
Version 5.x	FireSIGHT System or FireSIGHT Management Center (FMC)
Version 6.x	Firepower System or Firepower Management Center (FMC)

FireSIGHT:

- Cisco, after Sourcefire acquisition in 2013, rebranded the Sourcefire technologies.
- It's really a bit confusing because FireSIGHT is a new term introduced in version 5.
- FireSIGHT is a new term introduced in version 5 which to serve as a NGIPS/NGFW.
- In version 5, RNA and RUA combined together into a new term, which is FireSIGHT.
- Term FireSIGHT, it's mean we referred to entire system either physical or a virtual.

Old	New
Sourcefire	Cisco
Sourcefire Defense Center	FireSIGHT Management Center (FMC)
Sensor	Device or Managed Device
Defense Center (DC)	FireSIGHT Management Center
Sourcefire 3D System	FireSIGHT System
Sourcefire Managed Device	Managed Device

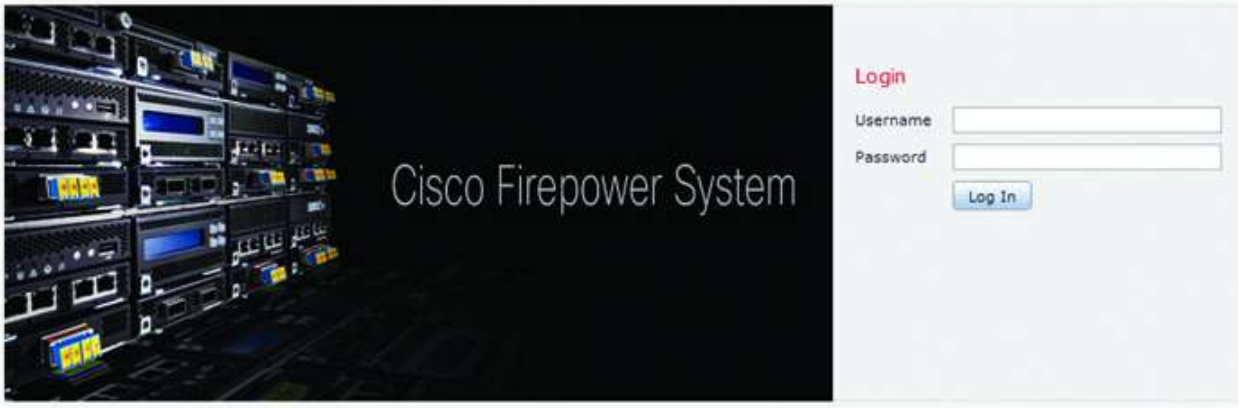


Firepower:

- When they updated to version 6.x, they changed the name to the current FirePOWER.
- Cisco uses FirePOWER (uppercase POWER) referring to Cisco ASA FirePOWER Services.
- Uses Firepower (lowercase power) referring to FTD unified image and newer software.
- Cisco introduced the Cisco ASA FirePOWER module as part of integration of Sourcefire.
- Firepower run as software module to complement ASA software on compatible devices.
- Firepower run as software module in ASA, approach is known as Firepower services.
- Firepower is the term Cisco uses for most of the products acquired from Sourcefire.
- A Firepower System deployment primarily consists of two main types of appliances.
- Firepower System deployment is one management appliance and other is the sensor.
- Sensor inspects network traffic and sends any events to it's the management appliance.
- Management appliance, as name suggest manages all kind of security policies for sensor.

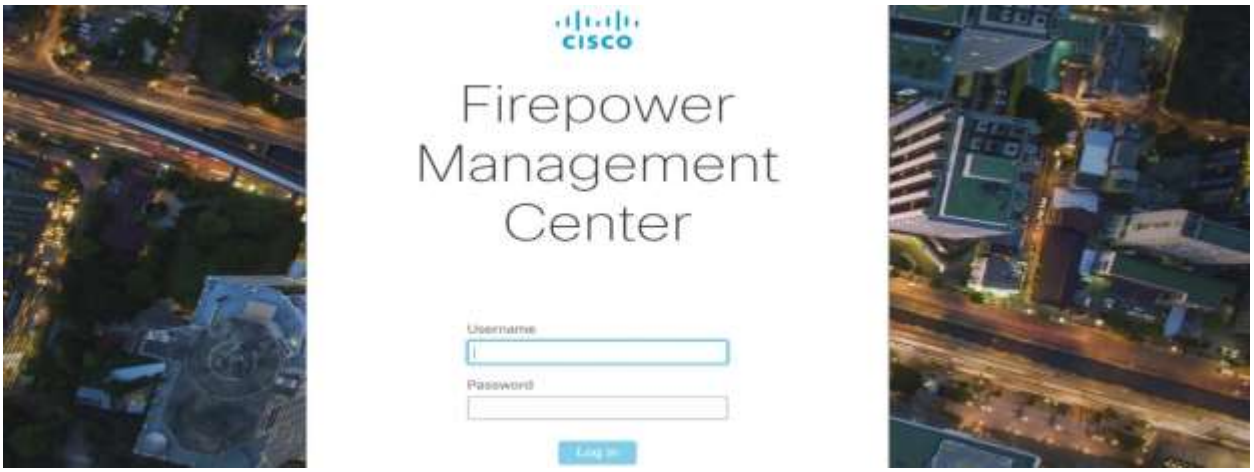
Firepower Thread Defense (FTD):

- Basically, the Firepower Threat Defense (FTD) is Cisco's Next-Generation firewall product.
- The FTD can be managed centrally by the Firepower Management Center (FMC) or FDM.
- Firepower Device Manager (FDM) through the on-box approach to access FTD Firewall.
- Cisco introduces Next-Generation security technologies in a unified FTD software image.
- The FTD offers Next-Generation, Next Generation Intrusion Prevention System and (AMP).
- The Firepower Threat Defense (FTD) offer all technologies in one single software solution.
- FTD is a unified software image, which includes Cisco ASA features & FirePOWER Services.
- This unified software is capable of offering function of ASA & FirePOWER in one platform.



Firepower Management Centre (FMC):

- The Managers provide a centralized management console with graphical user interface.
- That you can use to perform administrative, management, analysis, and reporting tasks.
- A separate physical or virtual appliance that can manage one or more Firepower devices.
- Cisco ASA FirePOWER module can be managed by Firepower Management Center (FMC).
- FMC provides very detailed analytics and statistics of what's happening in your network.



Next-Generation Firewall (NGFW):

- NGFW performs the role of a traditional firewall and adds the NGIPS features.
- Next-Generation Firewall is part of the third generation of Firewall technology.
- All NGFWs offer two key features App Awareness and Control & ID Awareness.
- Next-Generation Firewall (NGFW) provide deep-packet inspection of the traffic.
- Next-Generation Firewall add application-level inspection & Intrusion Prevention.
- Next-Generation Firewall provides all traditional IPS features with high performance.
- Next-Generation Firewall allow, and block traffic based on specific application as well.
- Next-Generation Firewall allow, and block traffic based on user information as well.
- Next-Generation Firewall (NGFW) provide both IPS and application control functions.
- There is no big difference between the UTM and Next-Generation Firewall (NGFW).
- Next-Generation Firewall provide high performance and Processing using to protect.