Cisco Firepower® QuickStart Implementation

Why Skyline Advanced Technology Services?

Skyline Advanced Technology Services (ATS) offers Professional Services for a variety of Cisco® centric solutions. From inception to realization, our senior staff of engineers are available for any size project or duration for the following services:

- Consulting Services
- Installation Services
- Network Design
- Staff Augmentation

For an in-depth discussion regarding your technical and staffing needs, our team is with you every step of the way.

Are you deploying FirePower?

Contact your Skyline-ATS Account Manager today for more information on how we can help.

800-375-9546
info@skyline-ats.com

Description

The Cisco Firepower® QuickStart Implementation is a unique Skyline-ATS onsite offering designed to assist partners/customers who are new to the Cisco FirePower solution. A dedicated Skyline-ATS FirePower Engineer is assigned to the partner's/customer's site location for the 4-day QuickStart implementation. The engagement is focused on the initial design, preparation of the partner's/customer's existing infrastructure, installation, and deployment of an operational FirePower system. The intended audience is IT personnel who not only need deployment services, but also need a well-defined knowledge transfer on FirePower.

Bundle the FirePower QuickStart with an ASA installation or ASA conversion to take advantage of business continuity and additional cost savings!

Overall Objectives

- Collaborate with key personnel to design and determine functionality goals.
- Interactive training and design sessions geared to finalize the design and educated the partner/customer.
- Cisco FireSIGHT™ Management Center (FMC) installation, including connectivity and management of FirePower devices.
- Creation and implementation of Access Policies (URL filtering), IPS policies, and AMP policies.
- Ensuring that the installation is successful by testing and verifying the new policies.

Prerequisites:

- For a physical appliance FMC – proper power, HVAC, cabling and other infrastructure.
- For a virtual appliance FMC – minimum of 8GB of RAM, with 4 CPUs, and 300GB of HDD space in an existing VMWare® environment.
- Familiarity with basic security practices and policies.
- Basic understanding of ASA firewalls.

Who Should Purchase this QuickStart?

- Security administrators
- Systems/Network engineers

Partner/Customer Responsibilities:

- A Bill of Materials (BOM) and Design Overview pre-installation.
- The personnel and ability to modify the network, firewalls, VMWare, and AD/RADIUS/TACACS environment as necessary.

Training Objectives

- Describe the FirePower system architecture, components, and options.
- Define connectivity requirements for the FMC and connectivity flows through the system.
- Define the differences between Access Policies, IPS policies, and AMP policies and how they are integrated.
- Describe the process of creating and integrating policies to secure the network.
- Describe the maintenance process.
- Identify connection flows through the system, including permissible or blocked connections.

FireSight Management Center

- Install licensing and management connectivity for up to two (2) FirePower modules.

FirePower Deployment

- Download all available updates (e.g., System patches, Geolocation Updates, IPS rules, etc.).
- Creation of an update schedule – may include immediate or delayed implementation of updates.
- Creation/Modification of a Health Policy.
- Creation/Modification of a System Policy.
- Creation and configuration of basic alerts.
- Creation/Modification of network discovery policy.
- Optional LDAP/Active Directory integration. Requires agent installation on AD domain servers. [time permitting].
- Optional RADIUS/TACACS integration. Requires a RADIUS or TACACS server. [Time permitting]
- Creation of a single and simple AMP policy.
- Creation of a single and simple IPS policy using recommended Cisco settings.
- Creation of a “wide open” policy to use as a fail safe.
- Creation of a single Access Control policy – may apply same policy to multiple devices.
  - Up to ten (10) rules.
  - Creation of up to ten (10) basic objects (e.g., networks, hosts, user groups, etc.).
  - Basic modification or redirection of custom response page.
- Testing of all basic rules and functionality.

Statement of Work

After a Skyline-ATS FirePower Engineer thoroughly qualifies the partner’s/customer’s FirePower requirements, a detailed Statement of Work (SOW) will be submitted for partner/customer approval prior to the QuickStart implementation engagement.

Disclaimer:

- Will not introduce malicious content to the network to test/verify IPS and AMP functionality.
- FirePower modules may include physical appliances or ASA integrated modules.
- IPS and AMP services cannot intercept and analyze encrypted traffic (HTTPS/SSH) on ASA modules. It is possible with appliances, but is beyond the scope of the QuickStart.
- ASA Firewall Deployment is NOT included in this QuickStart but may be added at additional time/cost.

Tentative Schedule

Day 1

Whiteboard Session 1 – Provide an overview of the FirePower components, a review of the connectivity and system requirements, information gathering. Plan for one (1) to two (2) hours.

- Topics to be discussed:
  - Cisco FireSIGHT™ Management Center
  - Cisco Powered™ Modules
  - Active Directory Integration (if applicable)
  - TACACS/RADIUS Integration (if applicable)
  - IP addressing
- Finalize IP addressing and design.
- Install Foresight Management Center.
- Register FirePower Modules to FMC.
- Install licensing.

Day 2

Whiteboard Session 2 – Provide an overview of the software components to FMC, upgrading the software and databases, how policies work in FMC. Plan for two (2) hours.

- Topics to be discussed:
  - Versioning for FMC, FirePower Modules, Geolocation Database, IPS database, etc.
  - Scheduling upgrades
  - Health Policies
  - System Policies
  - Network Discovery Policy
  - Access Policies with URL, IPS, and AMP integration
- Upgrade software components.
- Set a schedule for software upgrades.
- Create initial system and health policies.
- Integrate with RADIUS/TACACS.
- Integrate with Active Directory.
- Create initial baseline rule.

Day 3

Whiteboard Session 3 – Provide an overview of how URL, IPS, and AMP policies are applied. Plan for one (1) to two (2) hours.

- Topics to be discussed:
  - Access Policies
  - IPS Policies
  - AMP Policies
  - Objects/Targets
  - Whitelist/Blacklist
- Create initial:
  - Objects/Targets
  - Bbaseline rule
  - IPS rules
  - AMP rules
- Demonstrate how/why someone or something is being blocked or permitted access.

Day 4

- Review of initial rules.
- Modification of initial rules to better fit the organization.
- Setting up alerting.