Cisco ASA Next Gen Firewall with FirePOWER Services Technical Workshop

Duration: 2 Days **Course Code: GKASA5500X** **Version: 1.0** **Delivery Method: Company Event**

Overview:

Multifaceted, highly dynamic applications and bring-your-own-device (BYOD) workplaces have become the norm. And with them comes the challenge to balance productivity with security
Cisco has the industry's first adaptive, threat-focused next-generation firewall (NGFW) designed for a new era of threat and advanced malware protection. Cisco ASAs with FirePOWER Services deliver an integrated threat defense across the entire attack continuum — before, during, and after an attack. It combines the proven security capabilities of the ASA Firewalls with industry-leading Sourcefire threat and advanced malware protection features in a single device. This extends the capabilities of the Cisco ASA 5500-X Series beyond what other NGFW solutions provide.
Cisco ASA Next-Generation Firewall FirePOWER Services (SFR) Module addresses these needs by integrating the next-generation intrusion prevention system (NGIPS), application visibility & control (AVC), reputation- and category-based URL filtering and advanced malware protection (AMP) capabilities from Sourcefire. This integrated approach with multilayer protection gives much greater visibility into what's going on in your network. With full contextual awareness you will see all the resources.
Cisco FireSIGHT Management Center is the central management Center for all Sourcefire security solutions. The FireSIGHT Management Center lets you see and correlate extensive amounts of event data – applications, users, devices, operating systems, vulnerabilities, services, processes, files and threats – so you can get the complete picture of your network.
The FireSIGHT Management Center provides automated event impact assessment, policy tuning, policy management, and network and user behaviour analysis.
The results are end-to-end network intelligence and streamlined security operations. The time between detection and cure quickly shrinks in a streamlined operation.
This 2 -day workshop is designed to help users understand the integration of the SourceFire Security Suite with the Cisco ASA, FIreSIGHT and CSM for a new adaptive, threat-focused NGFW solution. You should at the end of this workshop feel confident in demonstrating the capabilities of the Cisco ASA Next-Generation Firewall FirePOWER Services(SFR) Module to potential customers.

Target Audience:

This course is intended for: Presales Consultants, System Engineers and Field Engineers.

Objectives:

- **After attending this course you should be able to:**
- Understand the capabilities of the FirePOWER Services Modules
- Install and configure the FirePOWER Services Module
- Explore the FireSIGHT Management Center using the Context Explorer
- Use Access Control,File Policies and Intrusion Policies to control traffic within a network
- Analyse files to determine their leavel of threat and trajectory within a network
- Integrate Active Directory with FireSIGHT and SourceFire User Agent for User based policies

Prerequisites:

Attendees should meet the following prerequisties:

- CCNA Certified preferably CCNA Security Certified.

Testing and Certification

Recommended training for exams:

- No exams are currently aligned to this course

Content:

Introducing the New Mid-Range Cisco ASAs and their Next Generation Firewall Services

- ASA FirePOWER - Benefits and Components
- ASA FirePOWER - Licensing
- Protection
- Control
- URL Filtering
- Malware
- Intrusion Prevention

Installing, Configuring and Integrating the ASA FirePOWER Services (SFR) module within an existing ASA

Using the Cisco Security Manager (CSM) to cross-launch the FireSIGHT Management Center

Exploring the FireSight Management Center

- Verify the licenses
- Add the ASA FirePOWER Services (SFR) Module

Edit and apply the initial system policy time synchronization settings to SFR Module

Apply the initial health policy to the SFR Module

Configure SFR Policy for a default Inline Intrusion Policy to use the Secure over Connectivity base IPS policy

Configure SFR Default Access Control policy to use the required File and IPS policy

Create and test user based access control policies

Configure File Polices to block malware

Attempt malware file transfers to trigger the malware blocking File Policy rule

Observe the IPS and Malware events in the FireSight Management Center

Integrate FireSIGHT with Microsoft Active Directory using the SourceFire User Agent for user and user-group based policies

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.be