SAEXS (CISCO ASA EXPRESS SECURITY)

Objetivo

Este curso foi concebido para a compreensão do portfólio de soluções da Cisco em ASA NGFW Firewall. Neste curso os alunos serão capacitados para configurar com sucesso vários aspectos dos componentes do produto, incluindo Cisco ASA Firewall, VPN Remote Access VPN para acesso remoto abrangendo a tecnologia SSL VPN com portal (Clientless) e com software cliente VPN (AnyConnect), e a integração com o módulo Firepower. Depois de concluir este curso, os alunos serão capazes de: • Descrever a tecnologia presente no Cisco ASA NGFW; • Configurar a integração do ASA NGFW junto à rede; • Selecionar, configurar e solucionar problemas de segurança de acordo com as características do equipamento; • Configurar e integrar o módulo Firepower ao ASA e ao gerenciador FireSight; • Descrever como configurar o Cisco ASA NGFW com soluções envolvendo AVC; • Configurar políticas do ASA NGFW utilizando objetos (host, redes, serviços e protocolos); • Descrever as características do Cisco's ASA Cloud Web Security; • Implementar solução de VPN para acesso remoto; • Descrever configuração para alta disponibilidade Failover Active/Standby

Público Alvo

O público principal deste curso são os responsáveis em projetar, implantar e prestar suporte em segurança para o firewall ASA NGFW.

Pré-Requisitos

Para aproveitar ao máximo este curso, é recomendável que os alunos possuam as seguintes habilidades e conhecimentos: • Conhecimentos básicos de rede; • Conhecimentos básicos de firewall; • Conhecimentos básicos de segurança; • Conhecimentos básicos de NAT, Inspeção de Aplicação e filtragem de pacotes (ACL´s); • Conhecimento do sistema operacional Microsoft Windows.

Carga Horária

16 horas (2 dias).

Conteúdo Programático

Firewall Technologies
• Overview about Firewall Technologies
• Cisco ASA Adaptive Security Appliance Features
• Cisco ASA Adaptive Security Appliance Hardware
Exploring Cisco ASA Connectivity Basics
• Preparing the Cisco ASA Adaptive Security Appliance for Network Integration
• Managing the Cisco ASA Adaptive Security Appliance Boot Process
• Managing the Cisco ASA Adaptive Security Appliance Using Cisco ASDM
• Navigating Basic Cisco ASDM Features

• Managing the Cisco ASA Adaptive Security Appliance Basic Upgrade
Managing Basic Cisco ASA Adaptive Security Appliance Network Settings
• Managing Cisco ASA Adaptive Security Appliance Security Levels
• Managing Basic Cisco ASA Adaptive Security Appliance Network Settings
• Configuring and Verifying Interface VLANs
• Configuring a Default Route
Configuring Cisco ASA Adaptive Security Appliance Routing Features
• Static Routing
• Dynamic Routing
• EIGRP Configuration and Verification
Backing up and Restoring Cisco ASA
• Cisco ASA Backup and Restore Overview
• Cisco ASA Backup – Configuring
• Cisco ASA Restore – Configuring
Configuring ASA Basic Access Control Foundation
• Configuring Cisco ASA Adaptive Security Appliance NAT Features
• NAT on Cisco ASA Security Appliances
• Configuring Object (Auto) NAT
• Configuring Manual NAT
• Configuring and Verifying Public Servers
• Tuning and Troubleshooting NAT on the Cisco ASA Adaptive Security Appliance
Configuring Cisco ASA Basic Access Control Features
• Connection Table and Local Host Table
• Configuring and Verifying Interface ACLs
• Configuring and Verifying Global ACLs
• Configuring and Verifying Object Groups
• Configuring and Verifying Other Basic Access Controls
Deploying Cisco Remote Access VPN
• Deploying Basic Clientless VPN Solutions
• Cisco ASA Clientless SSL VPN Solution
• Configuration Choices and Configuration Procedure
• Configuring Basic Cisco ASA Adaptive Security Appliance Gateway Features and
• Gateway Authentication
• Configuring Basic User Authentication
• Configuring Basic Access Control
• Tuning Gateway Content Rewriting
Cisco AnyConnect SSL VPN Overview
• Introduction to Cisco AnyConnect Client
• Cisco AnyConnect Client Core Features
• Cisco AnyConnect Network Access Manager
• Cisco AnyConnect Secure Mobility Modules
• Cisco AnyConnect Secure Reporting and Troubleshooting Modules
• Cisco AnyConnect Secure Mobility Licensing
Deploying a Cisco AnyConnect Client SSL VPN Solution
• Basic Cisco AnyConnect SSL VPN
• Additional Cisco AnyConnect Deployment Options
• Configuring Cisco ASA Gateway Features
• Configuring Local User Authentication and IP Address Assignment

- Configuring Access Control and Split Tunneling
- Deploying DTLS
- Installing and Configuring Cisco AnyConnect 3.X
- Managing Cisco AnyConnect Software

Introducing the Cisco ASA FirePower Services (SFR) Module

- NGFW Security Features
- Introducing Cisco ASA with FirePower Services (SFR) Module
- Cisco ASA FirePower Services (SFR) Module Overview
- Cisco FireSight Management Center Overview
- ASA 5506-X and 5508-X Overview
- Cisco ASA FirePower Services Module Management Interface
- Cisco ASA FirePower Services Module Package Installation
- Redirect Traffic to Cisco ASA FirePower Services Module
- Cisco ASA Firepower Services Module Verification

Cisco FireSight Management Center

- Firesight Management Center Virtual Machine Installation and Setup
- Add The Firepower Services Module into FireSight
- Firepower Services Module and FireSight License Requeriments
- FireSight Policy Types Overview
- System Policy Overview
- Health Policy Overview
- Tasks Status Monitoring
- Object Management Overview
- Security Zones Overview
- Network Discovery Overview
- Active Directory Integration Overview
- SourceFire User Agent Overview
- Access Control Policy Overview
- Intrusion Policy Overview
- FireSight Recommended Rules Overview
- File Policy Overview
- Indication of Compromise Overview
- Connection Events Monitoring
- Events Display Time Range
- Switch Workflow
- Intrusion Event Impact Levels Overview
- IPS Events Monitoring
- File Events Monitoring
- Users Monitoring
- Context Explorer
- Dashboards
- System Updates

Introducing Cisco ASA with Cisco Cloud Web Security

- Cisco ASA with Cisco Cloud Web Security
- Cisco Cloud Web Security URL Filtering, AVC and Reporting Features Overview
- Cisco Cloud Web Security Scanning Processes and Day Zero Outbreak Intelligence Overview
- Cisco ScanCenter
- Cisco ASA Cloud Web Security Licenses

Configuring Cisco ASA with Cisco Cloud Web Security
• Cisco ASA and Cloud Web Security Proxy-Server Configuration
• ScanCenter Generation of an Authentication Key for Cisco ASA
• Cisco ASA and Cloud Web Security Proxy Server User-Identity Configuration
Verifying Cisco ASA Cloud Web Security Operations
• Cisco ASA Cloud Web Security Operations Verification using the CLI
• Cisco ASA Cloud Web Security Operations Verifications using Cisco ASDM
• Verification of Traffic Redirection from Cisco ASA to Cloud Web Security Proxy Servers
• Cisco ASA Cloud Web Security Syslog Messages
• Cisco ASA Cloud Web Security Operations Verification using the debug scansafe CLI command
Describing the Web Filtering Policy in Cisco ScanCenter
• ScanCenter Web Filtering Policy Overview
• ScanCenter HTTPS Inspection Configuration Overview
• ScanCenter Web Filtering Reporting
Describing Cisco ASA Cloud Web Security AMP and CTA
• Cisco ASA CWS Advanced Malware Protection Overview
• Cisco Cloud Web Security Cognitive Threat Analytics
• Cisco ASA Cloud Web Security ScanCenter Threats Reporting Overview
Overview of Cisco ASA Active/Standby High Availability
• Cisco ASA Adaptive Security Appliance Active/Standby Failover Overview
• Active Unit Election
• Switchover Event
• Failover Management
• Failover Deployment Options
Configuring Cisco ASA Adaptive Security Appliance Active/Standby High Availability
• Configuring and Verifying Active/Standby Failover
• Tuning and Managing Active/Standby Failover
• Remote Command Execution

Roteiro de Laboratórios
Lab 1: Preparing ASA: Network Integration and Configuring Basic Settings
Lab 2: Configuring NAT and Basic Access Control
Lab 3: Configure Cisco AnyConnect Client SSL VPN Solution
Lab 4: Cisco ASA 5500-X FirePower Services (SFR) Module Installation and Setup
Lab 5: Cisco FireSight Management Center Configuration
Lab 6: Cisco ASA and Cloud Web Security Integration (Optional)