

# SENSS (IMPLEMENTING CISCO EDGE NETWORK SECURITY SOLUTIONS) 1.0

## Objetivo

Implementing Cisco Edge Network Security Solutions (SENSS) versão 1.0 é um treinamento que faz parte da grade de certificação CCNP Security. Além disso, tem como objetivo preparar os engenheiros de segurança para configurar e implantar segurança em equipamentos Cisco de perímetro, tais como switches, roteadores e o ASA Firewall. O objetivo do curso é proporcionar aos alunos o conhecimento fundamental e as capacidades para implantar e gerenciar segurança em Cisco ASA Firewalls, roteadores Cisco com o conjunto de recursos para firewall e switches Cisco. O aluno vai ganhar experiência “hands-on” com a configuração de várias soluções de segurança de perímetro para mitigar ameaças externas e garantir zonas de rede seguras. No final do curso, os alunos serão capazes de reduzir o risco de suas infraestruturas de TI e aplicações usando Switches Cisco, Cisco ASA, e característica de segurança do roteador e prestar suporte nas operações desses produtos. Depois de concluir este curso, os alunos serão capazes de: Compreender panorama atual das ameaças à segurança de rede; Compreender e implantar soluções da arquitetura modular em segurança da Cisco “SecureX” e “TrustSec”; Compreender e implantar as melhores práticas em segurança nos planos de gerência e controle da arquitetura Cisco (Management Plane e Control Plane); Compreender e implantar as melhores práticas em segurança no plano de dados (Data Plane) nos mecanismos em camada 2 e 3; Implantar e prestar suporte nas configurações de NAT do Cisco ASA Firewall e do roteador Cisco; Projetar e implantar soluções de segurança da arquitetura “Cisco Threat Defense” no Cisco Asa Firewall; Implantar e prestar suporte em configuração de inspeção protocolar no ASA Firewall (AIC Application Inspection Control); Implantar a solução Cisco Botnet no Cisco ASA Firewall; Implantar e configurar soluções em firewall baseada na arquitetura em zonas de rede (ZBFW Zone Based Firewall) em conjunto com as ferramentas em inspeção protocolar (AIC Application Inspection Control) nos roteadores Cisco

## Público Alvo

O público principal deste curso são os responsáveis em projetar, implantar e prestar assistência e suporte em segurança. Esse curso faz parte dos cursos preparatórios para a certificação CCNP Security.

## Pré-Requisitos

Para aproveitar ao máximo este curso, é recomendável que os alunos possuam as seguintes habilidades e conhecimentos: Ter participado no curso ICND1 ou possuir conhecimentos equivalentes em conceitos básicos de rede; Ter participado no curso IINS (CCNA Security) ou possuir conhecimentos em conceitos básicos de segurança abrangidos pelo curso; Conhecimento do sistema operacional Microsoft Windows

## Carga Horária

40 horas (5 dias).

## Conteúdo Programático

- Secure Design Principles
- Network Security Zoning
- Network Security Zones Implementation Model
- Cisco Modular Network Architecture Designs
- Cisco SecureX Architecture and Components
- Cisco TrustSec Architecture and Components

- Network Infrastructure Protection Deployment
- Introducing Cisco Network Infrastructure Protection
- Overview of Cisco Network Infrastructure Protection
- Identify Network Device Planes
- Control Plane Security Controls
- Management Plane Security Control
- Network Telemetry (NTP, Logging and Netflow)
- Layer 2 Data Plane Security Controls
- Layer 3 Data Plane Security Controls
- Deploying Cisco IOS/ASA Control Plane Security Controls
- Deploying Cisco IOS/ASA Management Plane Security Control
- Configure Cisco IOS/ASA Management Access AAA

- Deploying Cisco IOS Layer 2 Data Plane Security Controls
- Configure PVLANS (Private Vlans)
- DHCP Control and Configure DHCP Snooping
- ARP Control and Configure DAI (Dynamic ARP Inspection)
- Storm Control Overview
- MACSec Encryption

- Deploying Cisco Layer 3 Data Plane Security Controls
- Infrastructure Antispoofing
- Configure IP Source Guard

- NAT Deployment on Cisco IOS Software and Cisco ASA
- Overview of Network Address Translation
- Cisco Modular Network Architecture and Network Address Translation
- Inside and Outside NAT
- Static and Dynamic NAT
- NAT and PAT
- Policy-based NAT
- NAT and Cisco Products and Features
- Configure ASA Network Object NAT
- Configure ASA Manual NAT

- Threat Controls Deployment on Cisco ASA
- Overview of Firewall Threat Controls

Cisco Modular Network Architecture and Firewall Threat Controls  
Firewall Filtering Layers and Technologies  
Combining Firewall Filtering Technologies  
Firewall Threat Controls and Cisco Products and Features

Deploying Basic Cisco ASA Access Policies  
Connection Table  
Local Host Table  
Interface ACLs  
Global ACLs  
Object Groups  
Troubleshoot ACLs

Deploying Advanced Cisco ASA Access Policies  
Advanced Cisco ASA Access Policies Overview  
Cisco MPF (Modular Policy Framework) Overview  
OSI Layer 3 and 4 Policies Overview  
Support for Dynamic Protocols  
HTTP Inspector Overview  
FTP Inspector Overview  
Evaluate Application Inspection of Other Protocols

Deploying Reputation-Based Cisco ASA Access Policies  
Overview of the Cisco Botnet Traffic Filter  
Configure the Cisco Botnet Traffic Filter

Deploying Identity-Based Cisco ASA Access Policies  
Overview of the Identity Firewall and CDA  
Identity Firewall Flow  
Integrate Cisco CDA with AD and Cisco ASA  
Configure Identity-Based Access Rules Deploying Basic Cisco IOS Zone-Based Policy Firewall Access Policies  
Configure Zones and Zone Pairs  
Configure a Basic OSI Layer 3 and 4 InterZone Access Policy  
Configure a Basic OSI Layer 3 and 4 IntraZone Access Policy  
Configure Inspection of Control Plane and Management Plane Traffic  
Tune Stateful Engine and Connection Settings  
Configure Support for NAT  
Troubleshoot the Zone-Based Policy Firewall

Deploying Advanced Cisco IOS Zone-Based Policy Firewall Access Policies  
Overview of Advanced Access Policies  
Overview of Application-Layer Access Policies  
HTTP Inspector  
Inspection of Instant Messaging  
Inspection of Peer-to-Peer Protocols  
Additional Application Inspection  
URL Filtering Methods in Cisco IOS Zone-Based Policy Firewall  
Configure Local List-Based URL Filtering

## Roteiro de Laboratórios

- Lab 2-1: Configure Control and Management Plane Security Controls
- Lab 2-2: Configure Traffic Telemetry Methods
- Lab 2-3: Configure Layer 2 Data Plane Security Controls
- Lab 2-4: Configure Layer 3 Data Plane Security Controls
- Lab 3-1: Configure Cisco ASA NAT
- Lab 3-2: Configure Cisco IOS Software NAT
- Lab 4-1: Configure Basic Cisco ASA Access Policies
- Lab 4-2: Configure Advanced Cisco ASA Access Policies
- Lab 4-3: Configure Cisco ASA Botnet Traffic Filte
- Lab 4-4: Configure Cisco ASA Identity Firewall
- Lab 5-1: Configure Basic Cisco IOS Zone-Based Policy Firewall Access Policies
- Lab 5-2: Configure Advanced Cisco IOS Zone-Based Policy Firewall Access Policies