

# NGIPS (IMPLEMENTING IPS (SOURCEFIRE) FIREPOWER&FIRESIGHT AND INTEGRATION NGFW ASA) 1.0

## Objetivo

Este treinamento teórico e prático apresenta a solução de segurança Cisco NGIPS, abrangendo os produtos Cisco FirePOWER, Cisco FireSIGHT e a solução integrada Cisco ASA NGIPS Firepower. São abordados conceitos, a arquitetura, o desenvolvimento de projetos e implementações de soluções envolvendo os produtos, desde a sua instalação, integração a rede, atividades de configuração, operação e manutenção. São também abordadas as opções de alta disponibilidade e sua integração de rede. O aluno irá adquirir experiência prática para realizar configurações, e também vai aprender a verificar e monitorar o bom funcionamento de uma variedade de recursos, tais como funções de administração, funções de operações como a política de controle de acesso, implantação e configuração das funções de IPS, inspeção de arquivos, configurar objetos e a sua utilização em regras, configurações para filtragem de URL, assim como outras opções de operações.

## Público Alvo

Recomentado para profissionais que buscam conhecimentos na Implementação da solução Cisco NGIPS baseado nos produtos Cisco Firepower, Cisco FireSight e Cisco ASA NGIPS (ASA Firepower Module).

## Pré-Requisitos

Certificação CCNA ou conhecimentos equivalentes Conhecimentos básicos de segurança; Conhecimentos básicos do ASA Firewall (para alunos que vão integrar Cisco SourceFire Asa Module).

## Carga Horária

32 horas (4 dias).

## Conteúdo Programático

IPS Basics  
Managing Risk  
Risk Analysis  
Intrusion Prevention Terminology  
IDS x IPS  
IPS and Firewall Together

IPS Threats: IPS Features and Limitations

Network IPS Evasion Techniques  
Traffic Fragmentation  
Traffic-Level Misinterpretation  
Timing Attacks  
Encryption and Tunneling  
Resource Exhaustion  
Common Evasion Tools

IPS Architecture: Network IPS Products

IPS Architecture: Network IPS Approaches  
Signature Based  
Anomaly Based  
Policy Based  
Reputation Based  
Stateful Content Matching  
Protocol Decoding  
Packet Correlation  
Rate Analysis  
Packet Header Matching  
Packet Content Matching

IPS Architecture: Network IPS Traffic Analysis Methods  
Statistical Modeling  
Event Correlation  
Blended Threats  
Endpoint Security Controls  
System Approach to Security  
IPS Recommended Practices

IPS Architecture: IPS Deployment  
Sensor Deployments Considerations  
Security  
Protocol Decoding  
IDS (Detection) x IPS (Prevention)  
Performance  
Virtualization Policies

IPS Deployment: Implementing Network IPS At Enterprise Internet Edge  
Architecture Example  
DMZ Architecture Example  
Firewall Integration  
Design Guidelines

IPS Deployment: Implementing Network IPS At WANs  
Centralized Deployment  
Distributed Deployment  
Design Guidelines

IPS Deployment: Implementing Network IPS in Data Centers  
Architecture Example

IPS Deployment: Implementing Campus Sensor Deployment  
Centralized Sensors Clusters  
Design Guidelines

IPS Deployment: Promiscuous Mode Deployment (IDS)  
Definition  
Benefits and Limitations  
Deployment Options: SPAN  
Deployment Options: RSPAN  
Deployment Options: Flow-Based SPAN  
Deployment Options: VACL Capture Ports  
Deployment Options: Router-Selective Capture  
Deployment Options: ASA Firewall  
Deployment Guidelines

IPS Deployment: Inline Deployment (IPS)  
Inline Interface Pair Deployment  
Inline VLAN Pair Deployment  
Selective Inline Analysis Deployment  
Deployment Guidelines

IPS Deployment: High Availability and Cisco IPS Deployments  
Overview  
Switching Based: STP  
Switching Based: EtherChannel  
Routing Based  
Load Sharing  
Filter Traffic Reduction

IPS Review  
Vulnerabilities and Exploits  
IPS  
Problems With Traditional IPS  
Ways To Deployment IPS  
IPS Deployment Locations

NGIPS  
Configuration Problem  
Organizational Problem  
Addressing The Configuration Problem  
Two Kinds Of Integration  
Building a Visibility Architecture  
Types o Visibility  
Threat & Breach  
Control

Event Horizon  
NGIPS Solution

Cisco & SourceFire  
Cisco FirePOWER Family  
About SourceFire  
Open Source Snort  
Market Leadership (Magic Quadrant)  
Talos Group  
New Security Model Cisco  
Better Together

Cisco NGIPS  
FireSight & FirePower  
Policies Structure  
Traffic Flows Types  
Centralized Event Management  
FireSight Management Advantages  
FirePower Events Data

Cisco FireAMP  
Advanced Malware Protection  
Cisco Options  
How It Works  
FireAMP Appliances

Cisco NGIPS Architecture  
Solution Architecture  
FireSight Instalation

ASA NGIPS Architecture  
Solution Architecture  
Sample Solution  
Packet Flow  
ASA Compatibility  
ASA & FireSight  
Redirect Traffic to Module Configuration  
Considerations

Management Cisco NGIPS  
FireSight  
FirePower Registration Process  
Device Properties  
Stack Configuration  
Clustered Configuration

Administration User Management  
User Accounts

## User Roles

- Add User Account (Local)
- User Escalation Option
- User External Databases

## Objects Management

- Overview
- Network Objects
- Security Intelligence
- Ports Objects
- Protocol ICMP
- Vlans
- URL Objects
- Applications Filters
- Security Zones
- Geolocation

## Access Control Policy

- Overview
- Configure Access Control Policy
- Advanced Options

## Management IPS Rules

- IPS Policies Configurations
- FireSight Rules Recommendation
- Configure Alerts

## Discovery Management

- Overview
- Configuration and Tuning

## Malware Protection

- Overview
- Network Malware Detection
- Files Lists
- Using Reports

## IPS Tuning

- Overview
- Tuning False Positives and Negatives
- Tuning Strategies
- Tuning Phases
- Tools
- Guidelines
- Incident Management

## FireSight Tuning Process

- FireSight Network Analysis Tuning

## Intrusion Event & Investigation

FireSight Reports  
Generating Reports

Correlations Analysis  
Events & Responses  
Remediations Actions

ASA NGIPS High Availability  
Deployment Modes  
Active & Standby  
Clustering  
Multi-Context  
Asymmetric Traffic  
Session Failover

ASA Projects  
Measuring  
Performance Impacts  
ASA Feature Guidance  
Sizing Guidance

ASA NGIPS Deployment  
Redirect Traffic

dCloud Cisco

ASA NGIPS POV

Labs  
Verifying the Product Licenses  
Viewing Events  
Creating User Accounts  
Escalating Permissions  
Working with an External User Account  
Testing the LDAP Authentication Object  
Creating Objects  
Creating a Basic Access Control Policy  
URL Filtering  
Including an IPS Policy in Access Control Rules  
Tuning the Network Discovery Detection Policy  
Viewing FireSIGHT Data  
User Discovery  
Creating a File Policy  
Creating an Intrusion Policy  
Enabling Include FireSIGHT Recommendations  
Implementing FireSIGHT Recommendations

Testing the Network Analysis Policy Settings  
Analyzing Events  
Tuning an Event  
Using Context Explorer  
Comparing Trends  
Creating a Correlation Policy Based on Connection Data  
Whitelists  
Working with Connection Data and Traffic Profiles