

- Network Device
- Network Host

*Work hard in silence,  
let your success be  
your voice.*



**Signellent**  
Technologies(I) Pvt Ltd.

## **Identity Management, Information Exchange, and Access Control**

- ISE scalability using multiple nodes and personas.
- Cisco switches & Cisco Wireless LAN Controllers for network access AAA with ISE.
- Cisco devices for administrative access with ISE
- AAA for network access 802.1X & MAB using ISE.
- Guest lifecycle management using ISE & Cisco Wireless LAN controllers
- BYOD on-boarding and network access flows
- ISE integration with external identity sources
- LDAP
- AD
- External RADIUS
- Provisioning of AnyConnect with ISE and ASA
- Posture assessment with ISE
- Endpoint profiling using ISE and Cisco network infrastructure including device sensor
- Integration of MDM with ISE
- Certificate-based authentication using ISE
- Authentication methods
  - EAP Chaining
  - Machine Access Restriction (MAR)
- Identity mapping on ASA, ISE, WSA, and FTD
- pxGrid integration between security devices WSA, ISE, & Cisco FMC
- Integration of ISE with multi-factor authentication
- Access control and single sign-on using Cisco DUO security technology

**Perform packet capture and analysis using Wireshark, tcpdump, SPAN, ERSPAN, and RSPAN**

**DNS layer security, intelligent proxy, and user identification using Cisco Umbrella**

**Web filtering, user identification, and Application Visibility and Control (AVC) on Cisco FTD and WSA.**

**WCCP redirection on Cisco devices**

### **Email security features**

- Mail policies
- DLP
- Quarantine
- Authentication
- Encryption

**HTTPS decryption and inspection on Cisco FTD, WSA and Umbrella**

**SMA for centralized content security management**

**Cisco advanced threat solutions and their integration: Stealthwatch, FMC, AMP, Cognitive Threat Analytics (CTA), Threat Grid, Encrypted Traffic Analytics (ETA), WSA, SMA, CTR, and Umbrella**

**CCIE  
Security**

## **Advanced Threat Protection and Content Security (20%)**

**AMP for networks, AMP for endpoints, and AMP for content security (ESA & WSA)**

**Detect, analyze, and mitigate malware incidents**



**Counsellor:**

+91 98674 76037  
+91 9769977502  
mumbai@signellent.in  
thane@signellent.in

**Borivali / Thane / Ahmedabad / Gurgaon**

Unit No.1, Chaphekar Wadi, Near Sheth G.H.  
High School, Borivali (E), Mumbai - 400 066.  
Tel: 022 28900895

Pitru Chhaya CHS, Office No 7, 2nd Floor, R. S. Road,  
Chendani, Behind Ashok Talkies, Thane (W),  
Maharashtra 400601.

**www.signellent.in**

# Course Highlights

## Perimeter Security and Intrusion Prevention

### Deployment modes on Cisco ASA and Cisco FTD

- Routed
- Transparent
- Single
- Multi-Context
- Multi-Instance

### Firewall features on Cisco ASA and Cisco FTD

- NAT
- Application inspection
- Traffic zones
- Policy-based routing
- Traffic redirection to service modules
- Identity firewall

### Security features on Cisco IOS/IOS-XE

- Application awareness
- Zone-Based Firewall (ZBFW)
- NAT

### Cisco Firepower Management Center (FMC) features

- Alerting
- Logging
- Reporting

### NGIPS deployment modes

- In-Line
- Passive
- TAP

### Next Generation Firewall (NGFW) features

- SSL inspection
- User identity
- Geolocation
- AVC

### Detect, and mitigate common types of attacks

- DoS/DDoS
- Evasion Techniques
- Spoofing
- Man-In-The-Middle
- Botnet

### Clustering/HA features on Cisco ASA and Cisco FTD

### Policies and rules for traffic control on Cisco ASA and Cisco FTD

### Routing protocols security on Cisco IOS, Cisco ASA and Cisco FTD

- Network connectivity through Cisco ASA and Cisco FTD
- Correlation and remediation rules on Cisco FMC

## Secure Connectivity and Segmentation

- AnyConnect client-based remote access VPN technologies on Cisco ASA, Cisco FTD, and Cisco Routers.
- Cisco IOS CA for VPN authentication
- FlexVPN, DMVPN, and IPsec L2L Tunnels
- Uplink and downlink MACsec (802.1AE)
- VPN high availability using
- Cisco ASA VPN clustering
- Dual-Hub DMVPN deployments
- Infrastructure segmentation methods
- VLAN
- PVLAN
- GRE
- VRF-Lite
- Micro-segmentation with Cisco TrustSec using SGT & SXP

## Infrastructure Security

### Device hardening techniques and control plane protection methods

- CoPP
- IP Source routing
- iACLs

### Management plane protection techniques

- CPU
- Memory thresholding
- Securing device access

### Data plane protection techniques

- uRPF
- QoS
- RTBH

### Layer 2 security techniques

- DAI
- IPDT
- STP security
- Port security
- DHCP snooping
- RA Guard
- VACL

### Wireless security technologies

- WPA
- WPA2
- WPA3
- TKIP
- AES

## Management plane protection techniques

- CPU
- Memory thresholding
- Securing device access

## Data plane protection techniques

- uRPF
- QoS
- RTBH

## Layer 2 security techniques

- DAI
- IPDT
- STP security
- Port security
- DHCP snooping
- RA Guard
- VACL

## Wireless security technologies

- WPA
- WPA2
- WPA3
- TKIP
- AES

## Monitoring protocols

- NetFlow/IPFIX/NSEL
- SNMP
- SYSLOG
- RMON
- eStreamer

## Security features to comply with organizational security policies, procedures, and standards BCP 38

- ISO 27001
- RFC 2827
- PCI-DSS

## Cisco SAFE model to validate network security design and to identify threats to different Places in the Network (PINs)

## Interaction with network devices through APIs using basic Python scripts

- REST API requests and responses
- HTTP action verbs, error codes, cookies, headers
- JSON or XML payload
- Authentication
- Data encoding formats
- JSON
- XML
- YAML

## Cisco DNAC Northbound APIs use cases

- Authentication/Authorization
- Network Discovery