Idee e Valori al servizio delle Aziende

FORTINET NSE4 NETWORK SECURITY PROFESSIONAL

Il Corso Fortinet NSE 4 unisce i corsi FortiGate Security e FortiGate Infrastructure per fornire ai partecipanti una conoscenza completa delle tecnologie di sicurezza informatica e della gestione di rete attraverso le soluzioni dell'ecosistema Fortinet. Durante il corso, i partecipanti apprenderanno come installare, configurare e gestire le soluzioni di sicurezza di Fortinet, tra cui il firewall FortiGate, la protezione degli endpoint, la gestione delle reti e molto altro ancora. Il corso copre una vasta gamma di argomenti, tra cui la sicurezza del perimetro, il controllo degli accessi, la protezione degli endpoint, la sicurezza wireless, la gestione delle politiche di sicurezza e altro ancora. Inoltre, il corso prepara i partecipanti alla Certificazione Fortinet Network Security Expert (NSE) 4, fornendo loro le competenze e le conoscenze necessarie per superare l'esame di certificazione.

DURATA DEL CORSO

5 giorni

DESTINATARI

Possono partecipare al corso tutti gli studenti.

PREREQUISITI

I partecipanti dovranno avere una conoscenza scolastica della lingua Inglese e competenze sistemistiche e di networking di base;

CONTENUTI

Il corso tratta i seguenti macro contentuti:

FortiGate Security

Introduction

- High-Level Features
- Identify the platform design features of FortiGate
- Identify features of FortiGate in virtualized networks and the cloud
- Understand FortiGate security processing units (SPU)
- Setup Decisions
- Identify the factory default settings
- Understand the FortiGate relationship with FortiGuard and distinguish between live queries and package updates
- Basic Administration
- Manage administrator profiles
- Manage administrative users
- Define the configuration method for administrative users
- Define and describe VDOMs
- Control administrative access to the FortiGate GUI and CLI
- Manage specific aspects of the network interfaces
- Describe VLANs and VLAN tagging
- Enable the DHCP and DNS services on FortiGate
- Fundamental Maintenance
- Backup and restore system configuration files
- Understand the restore requirements for plaintext and encrypted configuration files
- Identify the current firmware version
- Upgrade firmware
- Downgrade firmware

Firewall Policies

- Identify components of firewall policies
- Identify how FortiGate matches traffic to firewall policies
- Configuring Firewall Policies
- Restrict access and make your network more secure using security profiles
- Configure logging
- Managing Firewall Policies
- Identify policy list views
- Understand the use of policy IDs
- Identify where an object is referenced
- Best Practices and Troubleshooting
- Identify naming restrictions for firewall policies and objects
- Reorder firewall policies for correct matching
- Demonstrate how to find matching policies for traffic type

NAT

- Introduction to NAT
- Understand NAT and port address translation (PAT)
- Understand the different configuration modes available for NAT
- Firewall Policy NAT
- Configure a firewall policy to perform SNAT and DNAT (VIP)
- Apply SNAT with IP pools
- Configure DNAT with VIPs or a virtual server
- Central NAT
- Configure central NAT
- Best Practices and Troubleshooting
- Identify common NAT issues by reviewing traffic logs

- Best Practices and Troubleshooting
- Identify common NAT issues by reviewing traffic logs
- Monitor NAT sessions using diagnose commands
- Use NAT implementation best practices

Firewall Authentication

- Methods of Firewall Authentication
- Describe firewall authentication
- Identify the different methods of firewall authentication available on FortiGate devices
- Identify supported remote authentication servers
- Understand the roles of LDAP and RADIUS
- Describe active and passive authentication and order of operations
- User Groups
- Configure user groups
- Authentication Using Firewall Policies
- Configure firewall policies
- Monitor firewall users

Logging and Monitoring

- Log Basics
- Describe the log workflow
- Identify log types and subtypes
- Describe log severity levels
- Describe the layout of a log message
- Describe the effect of logging on performance
- Local and Remote Logging
- Identify log storage options
- Enable local and remote logging
- Understand disk allocation and reserved space
- Understand how remote logging works with VDOMs
- Understand log transmission
- Enable reliable logging
- Log Settings and Log Search
- Configure log settings
- Enable logging on firewall policies
- Hide user names in logs
- View and search for log messages
- Configure alert email
- Configure threat weight
- Protect Log Data
- Perform log backups
- Configure log rolling and uploading
- Perform log downloads

Certificate Operation

- Authenticate and Secure Data Using Certificates
- Describe why FortiGate uses digital certificates
- Describe how FortiGate uses certificates to authenticate users and devices
- Describe how FortiGate uses certificates to ensure the privacy of data
- Inspect Encrypted Data
- Describe certificate inspection and full SSL inspection
- Configure certificate inspection and full SSL/SSH inspection
- Identify what is required to implement full SSL inspection
- Identify the obstacles to implementing full SSL inspection and possible remedies

Web Filtering

- Inspection Modes
- Describe FortiGate inspection modes
- Review NGFW operation modes
- Web Filtering Basics
- Describe web filter profiles
- Work with web filter categories
- Additional Proxy-Based Web Filtering Features
- Configure web filter to support search engines
- Configure web content filtering
- Video Filtering
- Enable a YouTube API key
- Filter YouTube videos using FortiGuard
- Filter YouTube based on restriction level
- Filter YouTube channels
- Best Practices and Troubleshooting
- Understand HTTP inspection order
- Troubleshoot filter issues
- Investigate FortiGuard connection issues
- Apply web filter cache best practices
- Monitor logs for web filtering events

Application Control

- Application Control Basics
- Understand application control
- Detect types of applications
- Understand the FortiGuard application control services database
- Use application control signatures
- Application Control Configuration
- Configure application control in profile mode
- Configure application control in next generation firewall (NGFW) policy mode
- Use the application control traffic shaping policy
- Logging and Monitoring Application Control Events
- Enable application control logging events
- Monitor application control events
- Use FortiView to see a detailed view of application control logs
- Best Practices and Troubleshooting
- Recognize best practices for application control configuration
- Understand how to troubleshoot application control update issues

Antivirus

- Antivirus Basics
- Review antivirus scanning techniques
- Enable FortiSandbox with antivirus
- Differentiate between available FortiGuard signature databases
- Antivirus Scanning Modes
- Apply the antivirus profile in flow-based inspection mode
- Apply the antivirus profile proxy inspection mode
- Compare all available scanning modes
- Antivirus Configuration
- Configure antivirus profiles
- Configure protocol options
- Log and monitor antivirus events
- Best Practices
- Recognize recommended antivirus configuration practices
- Log antivirus events
- Monitor antivirus and FortiSandbox events
- Use hardware acceleration with antivirus scans
- Troubleshooting
- Troubleshoot common antivirus issues

Intrusion Prevention System and Denial of Service

- Intrusion Prevention System
- Differentiate between exploits and anomalies
- Identify the different components of an IPS package
- Manage FortiGuard IPS updates
- Select an appropriate IPS signature database
- Configure an IPS sensor
- Identify the IPS sensor inspection sequence
- Apply IPS to network traffic
- Denial of Service
- Identify a DoS attack
- Configure a DoS policy
- Best Practices
- Identify the IPS implementation methodology
- Enable full SSL inspection for IPS-inspected traffic
- Identify hardware acceleration components for IPS
- Troubleshooting
- Troubleshoot FortiGuard IPS updates
- Troubleshoot IPS high-CPU usage
- Manage IPS fail-open events
- Investigate false-positive detection

Security Fabric

- Introduction to the Fortinet Security Fabric
- Define the Fortinet Security Fabric
- Identify why the Security Fabric is required
- Identify the Fortinet devices that participate in the Security Fabric, especially the essential ones
- Deploying the Security Fabric
- Understand how to implement the Security Fabric
- Configure the Security Fabric on root and downstream FortiGate devices
- Understand how device detection works
- Understand how to extend your existing Security Fabric
- Extending the Security Fabric and Features
- Extend the Security Fabric across your network
- Understand automation stitches
- Configure external connectors
- Understand the Security Fabric status widgets
- Security Fabric Rating Service and Topology View
- Understand the Security Fabric rating service
- View and run the Fortinet Security rating service
- Understand the differences between physical and logical topology views

lFortiGate Infrastructure

Routing

- Routing on FortiGate
- Identify the routing capabilities on FortiGate
- Configure static routing
- Implement policy routes
- Route traffic for well-known internet services
- Routing Monitor and Route Attributes
- Interpret the routing table on FortiGate
- Identify how FortiGate decides which routes are installed in the routing table
- Identify how FortiGate chooses the best route using route attributes

- Equal Cost Multipath Routing (ECMP)
- Identify the requirements for ECMP routing
- Implement route redundancy and load balancing
- Reverse Path Forwarding (RPF)
- Identify how FortiGate detects IP spoofing
- Block traffic from spoofed IP addresses
- Differentiate between and implement the different RPF check methods
- Link Health Monitor and Route Failover
- Configure the link health monitor
- Implement route failover
- Use the forward traffic logs
- Diagnostics
- View active, standby, and inactive routes
- View policy routes on the CLI
- Use the built-in packet capture tool

Virtual Domains

- VDOM Concepts
- Define and describe VDOMs
- VDOM Administrators
- Create administrative accounts with access limited to one or more VDOMs
- Configuring VDOMs
- Configure VDOMs to split a FortiGate into multiple virtual devices
- Multi VDOM types
- Inter-VDOM Links
- Route traffic between VDOMs
- Best Practices and Troubleshooting
- Limit the resources allocated globally and per VDOM
- Troubleshoot common VDOM issues

Fsso

- FSSO Function and Deployment
- Define single sign-on (SSO) and Fortinet single sign-on (FSSO)
- Understand FSSO deployment and configuration
- FSSO With Active Directory
- Detect user login events in Windows AD using FSSO
- Identify FSSO modes for Windows AD
- FSSO Settings
- Configure SSO settings on FortiGate
- Install FSSO agents
- Configure the Fortinet collector agent
- Troubleshooting
- Recognize and monitor FSSO-related log messages
- Perform basic FSSO troubleshooting

Ztna

- ZTNA Introduction
- Understand the benefits of using ZTNA
- Understand the fundamentals of ZTNA
- Understand how to establish device identity and trust
- Understand SSL certificate-based authentication
- Configure ZTNA access on FortiOS
- Describe types of ZTNA configuration
- Comparing ZTNA to SSL and IPSec VPN
- Describe the differences between SSL VPN, IPsec VPN, and ZTNA access
- Understand the evolution of teleworker remote access with ZTNA

SSL Vpn

- SSL VPN Deployment Modes
- Describe the differences between SSL VPN modes
- Configuring SSL VPNs
- Define authentication for SSL VPN users
- Configure SSL VPN portals
- Configure SSL VPN settings
- Define firewall policies for SSL VPNs
- Configure client integrity check
- Monitoring and Troubleshooting
- Monitor SSL VPN-connected users
- Review SSL VPN logs
- Configure SSL VPN timers
- Troubleshoot common SSL VPN issues
- Identify hardware acceleration components for SSL VPN
- IPSec VPN
- IPsec Introduction
- Describe the benefits of IPsec VPN
- Be familiar with the IPsec protocol
- Understand how IPsec works
- Select an appropriate VPN topology
- IPsec Configuration
- Learn about the IPsec wizard
- Identify and understand the phases of IKE-v1
- Understand IPsec phase 1 and phase 2 settings
- Routing and Firewall Policies
- Understand route-based IPsec VPNs
- Learn how to configure routing and firewall policies for IPsec traffic
- Redundant VPNs
- Learn about redundant VPNs
- Understand redundant VPN configuration between two FortiGate devices
- Monitoring and Logs
- Learn how to monitor an IPsec VPN status
- Check IPsec VPN logs

High Availability

- HA Operation Modes
- Identify the different operation modes for HA
- Understand the primary FortiGate election in an HA cluster
- HA Cluster Synchronization
- Identify the primary and secondary device tasks in an HA cluster
- Identify what is synchronized between HA cluster members
- Configure session synchronization for seamless failover
- HA Failover and Workload
- Identify the HA failover types
- Interpret how an HA cluster in active-active mode distributes traffic
- Implement virtual clustering per VDOM in an HA cluster
- Monitoring and Troubleshooting
- Verify the normal operation of an HA cluster
- Configure an HA management interface
- Upgrade the HA cluster firmware

Diagnostics

- General Diagnosis
- Identify your network's normal behavior
- Monitor for abnormal behavior, such as traffic spikes
- Diagnose problems at the physical and network layers
- Debug Flow

Attività Laboratoriali

- Routing
- SD-WAN Configuration
- VDOM Configuration
- Transparent Mode Configuration
- Site-to-Site IPsec VPN Configuration
- Fortinet Single Sign-On (FSSO) Configuration
- High Availability (HA)
- Web Proxy Configuration
- Diagnostics Performance
- Introduction to FortiGate
- Security Fabric
- Firewall Policies
- NAT
- Firewall Authentication
- Logging and Monitoring
- Certificate Operations
- Web Filtering
- Application Control
- Antivirus
- Intrusion Prevention System (IPS) and Denial of Service (DoS)
- SSL-VPN
- Dialup IPsec VPN