



Cyberbezpieczny Samorząd

INW.271.3.P.2025

OPIS PRZEDMIOTU ZAMÓWIENIA – Załącznik nr 2 do Zapytania ofertowego

Dotyczy postępowania o udzielenie zamówienia publicznego pn.: **Zakup specjalistycznej usługi szkoleniowej dla pracownika IT Urzędu Miejskiego w Oławie z obsługi zakupionego sprzętu i oprogramowania służącemu zwiększeniu cyberbezpieczeństwa w ramach projektu pn.: „Wzmocnienie poziomu cyberbezpieczeństwa Urzędu Miejskiego w Oławie”**

1. FortiGate Administrator

Wymagania:

- czas trwania: 4 dni
- liczba uczestników: 1 osoba
- szkolenie w formie on-line
- szkolenie autoryzowane przez firmę Fortinet
- szkolenie prowadzone przez certyfikowanego trenera Fortinet w języku polskim
- materiały szkoleniowe w wersji elektronicznej

Program:

- System and Network Settings
- Firewall Policies and NAT
- Routing
- Firewall Authentication
- Fortinet Single Sign-On (FSSO)
- Certificate Operations
- Antivirus
- Web Filtering
- Intrusion Prevention and Application Control
- SSL VPN
- IPsec VPN
- SD-WAN Configuration and Monitoring
- Security Fabric
- High Availability
- Diagnostics and Troubleshooting

2. FortiAnalyzer Analyst

Wymagania:

- czas trwania: 1 dzień
- liczba uczestników: 1 osoba
- szkolenie w formie on-line
- szkolenie autoryzowane przez firmę Fortinet
- szkolenie prowadzone przez certyfikowanego trenera Fortinet w języku polskim
- materiały szkoleniowe w wersji elektronicznej

Program:

- Introduction and Initial Configuration
- Logging
- FortiSoC-Events and Incidents
- Reports
- FortiSoC-Playbooks



Fundusze Europejskie
na Rozwój Cyfrowy

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

3. Configuring AOS-S Switches Level 1

Wymagania:

- czas trwania: 3 dni
- liczba uczestników: 1 osoba
- szkolenie w formie on-line
- szkolenie autoryzowane przez firmę HPE/Aruba networking
- szkolenie prowadzone przez certyfikowanego trenera HPE/Aruba networking w języku polskim
- materiały szkoleniowe w wersji elektronicznej

Program:

- Introduction to HPE Aruba Networking
- Describe market trends that are causing customers to transform in four key transformation areas
- Describe how HPE Aruba Networking delivers the digital workplace.
- Switch CLI (Command Line Interface) navigation
- Describe out-of-band management
- Complete the initial setup on AOS-S switches
- Verify configuration
- Protecting management access
- Explanation of in-band management
- Protect in-band and out-of-band management access
- Configure local authentication
- Control the privilege level allowed to managers
- Management of software and configurations
- Overview of AOS-S and file structures
- Different methods for setting the software from which to boot
- Software update
- Saving and restoring configurations
- VLANs
- Explain use cases for VLANs
- Configure port-based VLANs on AOS-S switches, using appropriate tagging
- Implement basic IP routing between directly connected VLANs or links
- Spanning Tree Protocol (STP)
- Understand and configure Rapid Spanning Tree Protocol (RSTP)
- Understand how Multiple Spanning Tree Protocol (MSTP) provides load sharing and implement MSTP.
- Link aggregation
- Differentiate between different types of link aggregation and understand the benefits of Link Aggregation Control Protocol (LACP)
- Configure and troubleshoot link aggregation on AOS-S switches
- IP routing
- Configure static routes on AOS-S switches
- Interpret IP routing tables
- Configure a basic OSPF solution
- Virtual Switching Framework (VSF)
- Understand how VSF works and the advantages that it provides
- Configure and verify a simple VSF fabric
- Wireless for small-to-medium businesses (SMBs)
- Understand the basics of wireless communications and 802.11 standards
- Define a WLAN and differentiate between wireless security options



Fundusze Europejskie
na Rozwój Cyfrowy

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

- Configure basic settings on HPE Aruba Networking Instant Access Points
- Form an HPE Aruba Networking Instant cluster
- HPE Aruba Networking AirWave
- Configure AirWave management settings on an Instant AP cluster
- Configure SNMP v2c settings on AOS-S switches
- Discover AOS-S switches in AirWave and bring switches and Instant APs under monitoring and management
- Implement zero touch provisioning (ZTP) for Instant APs and AOS-S switches

4. Configuring AOS-S Switching Level 2

Wymagania:

- czas trwania: 5 dni
- liczba uczestników: 1 osoba
- szkolenie w formie on-line
- szkolenie autoryzowane przez firmę HPE/Aruba networking
- szkolenie prowadzone przez certyfikowanego trenera HPE/Aruba networking w języku polskim
- materiały szkoleniowe w wersji elektronicznej

Program:

- Introduction to Aruba Solutions
- Data Link Layer Redundancy Technologies
- Virtual Router Redundancy Protocol (VRRP)
- Aruba Backplane Stacking and Advanced Virtual Switch Framework (VSF)
- Advanced Open Shortest Path First (OSPF)
- Internet Group Management Protocol (IGMP)
- Border Gateway Protocol (BGP)
- Access Control Lists (ACLs)
- MAC Authentication
- Captive Portal and Other Guest Options
- Integrating with Aruba Mobility Solutions
- Secure Device Management
- Quality of Service (QoS)
- Additional Security Features

5. Implementing AOS-CX Switching

Wymagania:

- czas trwania: 5 dni
- liczba uczestników: 1 osoba
- szkolenie w formie on-line
- szkolenie autoryzowane przez firmę HPE/Aruba networking
- szkolenie prowadzone przez certyfikowanego trenera HPE/Aruba networking w języku polskim
- materiały szkoleniowe w wersji elektronicznej

Program:

- Intro to AOS-CX Switching
- AOS-CX switch overview
- Legacy management systems
- Modern management approach
- The REST API and URIs
- NAE and the Time-series database
- Dynamic Segmentation
- Always on POE



Fundusze Europejskie
na Rozwój Cyfrowy

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

- Virtual Output Queuing
- Virtual Switching eXtension
- Virtual switching technologies
- VSX components
- VSX synchronization
- Split brain scenarios
- Layer 2 Optimization
- UDLD
- Private VLAN
- Basics of Spanning Tree Protocol
- RPVST+
- Advanced OSPF
- OSPF overview
- Multi-area OSPF
- Route redistribution using ASBRs
- OSPF area types
- OSPF redundancy
- Additional OSPF features
- Border Gateway Protocol
- BGP overview
- BGP neighbor connections
- BGP route advertisements
- BGP route selection metrics and tuning
- Controlling eBGP routes
- Additional Layer 3 Features
- Virtual routing and forwarding (VRF)
- Policy-based routing
- ARP protection
- DHCP snooping
- IPsec and NAT
- IGMP
- Multicast introduction
- IGMP overview
- Multicast Routing
- PIM introduction
- PIM-DM
- PIM-SM
- PIM-SM build-up process
- BSR mechanism
- VSX and PIM
- Access Control Lists
- ACL introduction and creation
- ACL application scenarios
- Applying ACLs
- Object groups
- Classification policies
- Restrictions and resource utilization
- 802.1X Authentication



Fundusze Europejskie
na Rozwój Cyfrowy

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

- Authentication overview
- 802.1X authentication overview
- Configuring 802.1X on switch ports
- RADIUS attributes for the dynamic settings
- User roles overview
- Device fingerprinting overview
- MAC Authentication
- MAC authentication overview
- MAC-auth with multiple clients
- MACsec overview
- Dynamic Segmentation
- Dynamic Segmentation overview
- User-based tunneling
- Configuring UBT
- UBT with MC cluster
- Troubleshooting
- REST API
- REST API introduction
- REST basic concepts
- Enabling the REST interface on an AOS-CX switch
- Sending requests to the REST API
- Accessing the REST API reference interface
- Use cases and resources
- Quality of Service
- QoS overview
- Classifying traffic and applying policies
- LLDP-MED and device profiles
- Network Analytics Engine (NAE)
- NAE overview
- NAE agents
- Agent actions
- Troubleshooting
- Troubleshooting overview
- Troubleshooting principles
- Components of effective troubleshooting
- Need for a methodical approach
- Problem-solving methodology
- Network troubleshooting tools

6. Configuring HPE Aruba Networking ClearPass

Wymagania:

- czas trwania: 5 dni
- liczba uczestników: 1 osoba
- szkolenie w formie on-line
- szkolenie autoryzowane przez firmę HPE/Aruba networking
- szkolenie prowadzone przez certyfikowanego trenera HPE/Aruba networking w języku polskim
- materiały szkoleniowe w wersji elektronicznej

Program:

- Introduction to ClearPass



Fundusze Europejskie
na Rozwój Cyfrowy

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

- BYOD
- High level overview
- Posture and profiling
- Guest and Onboard
- AAA
- Policy service rules
- Authentication, authorization, and roles
- Enforcement policy and profiles
- External devices
- Network access devices
- Messaging services
- External context servers
- Endpoint profiling
- Introduction to profiling
- Profiling collectors
- External collectors and profilers
- Roles and enforcement
- Services
- Enforcement
- ClearPass roles
- Configuring services
- Service selection rules
- Creating services
- Configuring web services
- Content Manager
- Skins
- Web page editor
- Guest authentication
- Captive portal process
- Web logins
- Guest accounts
- Guest access with MAC authentication
- Guest access self registration
- Self registration experience
- Configuring self registration
- Self registration process
- Wired authentication
- Wired access
- Wired enforcement
- Profiling on wired ports
- Downloadable user roles
- Requirements for DUR
- DUR enforcement profiles
- Dynamic Segmentation
- What is Dynamic Segmentation?
- How it works
- Configuring Dynamic Segmentation
- ClearPass OnGuard Software configuration





Cyberbezpieczny Samorząd

- Postures
- Posture policies
- ClearPass OnGuard Software agent
- Monitoring ClearPass OnGuard Software
- ClearPass OnGuard Software in enforcement
- ClearPass OnGuard Software workflow
- ClearPass OnGuard Software enforcement
- ClearPass Onboard Software provisioning
- Configuring certificate authorities
- Portal setup
- Configuring services
- ClearPass Onboard Software Administration
- Managing certificates
- Managing users and devices
- Certificate revocation and OCSP
- Administrative operations
- Licenses
- Certificates
- Updates and upgrades
- Gathering logs
- ClearPass cluster
- Cluster structure
- Policy Manager zones
- High availability
- Administrative access
- Admin access to NADs
- Admin access to Policy Manager
- Guest operator logins
- ClearPass Device Insight reports
- Alerts
- Reports
- Administration

7. Veeam® Backup & Replication™ v12.1: Configure, Manage, and Recover (VMCE)

Wymagania:

- czas trwania: 4 dni
- liczba uczestników: 1 osoba
- szkolenie w formie on-line
- szkolenie autoryzowane przez firmę Veeam
- szkolenie prowadzone przez certyfikowanego trenera Veeam w języku polskim
- materiały szkoleniowe w wersji elektronicznej

Program:

- Data protection strategies
- Review of key data protection strategies that ensure the safety of your data.
- Analysis of risks to data
- Explore different risk scenarios - What risks do we face daily within our environment?
- What is protected?
- Review of Veeam Data Platform and introduction to the class scenario.
- Security and protection considerations



Fundusze Europejskie
na Rozwój Cyfrowy

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

- Describe strategies and tools to secure the Veeam backup server to avoid unauthorized access and data leaks.
- Protecting workloads
- Efficiently protect VMware and Hyper-V virtual machines based on well-defined SLAs through the creation of backup jobs.
- Deploying agents
- Identify the use of protection groups to automate the installation of Veeam Agents and protecting workloads with agent backup jobs.
- Unstructured data backup
- List required components and features available to protect unstructured data.
- Optimizing your backups
- Analyze features and settings that allow backup storage optimization, faster backups, and data consistency.
- Immutability and hardened repositories
- Describe backup data protection mechanisms to avoid premature deletion and unwanted modifications.
- Identify characteristics and deployment steps of Linux Hardened Repositories to achieve backup data immutability.
- Backup infrastructure optimization
- List deployment options and additional settings to improve general backup solution performance.
- Replication
- Describe use cases, architectures, and features of replication jobs and continuous data protection (CDP) policies.
- Backup copy jobs
- Ensure recoverability and adhere to the 3-2-1 Rule with backup copy jobs.
- Long-term retention
- List different mechanisms for data archiving, including grandfather-father-son retention policies.
- Scale-out Backup Repository™
- Describe architecture, placement policies, data tiers, and management of Scale-out Backup Repositories.
- Move and copy backups with Veeam Mover
- Identify use cases for virtual machine and backup migrations with Veeam Mover.
- Recovery verification
- Create automated tests to ensure recoverability from backups and replicas.
- Veeam Backup Enterprise Manager
- Describe the use cases for Veeam Backup Enterprise Manager.
- Incident Response Planning
- Integrating Veeam Backup and Replication into your incident response plan.
- Advanced recovery features
- Explore some more in-depth recovery features of Veeam Backup and Replication.
- Selecting the ideal recovery method
- What are the implications of different recovery methods and selecting the correct recovery method?
- Enacting a recovery
- Get practice in recovering different recovery types with a variety of data types.
- Lab 1: Secure Veeam backup server
- Lab 1.1: Secure the Veeam backup server
- Lab 2: Protect virtual machines





Cyberbezpieczny Samorząd

- Lab 2.1: Add the virtual infrastructure to the Veeam Backup & Replication inventory
- Lab 2.2: Protect virtual workloads
- Lab 3: Veeam Agent backup capabilities
- Lab 3.1: Automate deployment of Veeam Agents
- Lab 3.2: Protect physical workloads
- Lab 4: Unstructured data backup capabilities
- Lab 4.1: Prepare Veeam infrastructure for file share backups
- Lab 4.2: Protect file share workloads
- Lab 5: Backup infrastructure optimization
- Lab 5.1: Deploy a dedicated VMware backup proxy
- Lab 5.2: Deploy a Veeam Hardened Repository
- Lab 5.3: Deploy immutable object storage
- Lab 6: Second site backup and backup management
- Lab 6.1: Create a backup copy job
- Lab 6.2: Create a Scale-out Backup Repository (SOBR)
- Lab 6.3: Create a dynamic backup job
- Lab 6.4: Migrate virtual machine backups to another job
- Lab 7: Building replication capabilities
- Lab 7.1: Prepare Veeam infrastructure for virtual machine replication
- Lab 7.2: Working with replication jobs
- Lab 7.3: Working with CDP policies
- Lab 8: Testing virtual machine backups
- Lab 8.1: Create a SureBackup job to verify backups
- Lab 8.2: Create a SureBackup job to verify replicas
- Lab 9: Working with Veeam Backup Enterprise Manager
- Lab 9.1: Connect the backup server with Veeam Backup Enterprise Manager
- Lab 9.2: Decrypt an imported encrypted file
- Lab 9.3: Create a restore operator user
- Lab 10: Application items recovery
- Lab 10.1: Perform a Microsoft SQL Server instant database recovery
- Lab 10.2: Restore an Active Directory user
- Lab 11: Recovering a guest OS file
- Lab 11.1: Restore a guest operating system file
- Lab 11.2: Restore a guest operating system file with disk publishing
- Lab 12: Full virtual machines recovery
- Lab 12.1: Recover a virtual machine with Instant Recovery
- Lab 12.2: Recover a virtual machine with full VM recovery and quick rollback
- Lab 13: Restore a physical machine from an Agent backup
- Lab 13.1: Perform a bare metal recovery of a Windows physical machine from an Agent backup
- Lab 13.2: Perform an instant VM recovery of a Linux physical machine from an Agent backup
- Lab 14: Restore from a replica
- Lab 14.1: Disaster failover to a VMware vSphere® replica and failback to production
- Lab 14.2: Working with replica failover plans
- Lab 14.3: Planned failover to a Microsoft Hyper-V replica
- Lab 15: Restore from a file share backup
- Lab 15.1: Recover a file share folder from backup
- Lab 15.2: Recover an entire file share with instant file share recovery





Cyberbezpieczny Samorząd

Zamawiający wymieniając w niniejszym opisie nazwy własne programów lub urządzeń wskazuje, co używane jest w Urzędzie Miejskim w Oławie i w takim dedykowanym zakresie wymaga przeszkolenia.

Zamawiający wymaga wykonania szkolenia w najnowszej aktualnie dostępnej wersji. Jeżeli od momentu zapytania program szkolenia zostanie zaktualizowany przez firmę certyfikującą szkolenia, zamawiający akceptuje stosowne zmiany w oznaczeniach szkolenia i jego programie.

Termin realizacji szkoleń do dnia 31.12.2025. Termin każdego szkolenia powinien być uzgodniony i zaakceptowany przez zamawiającego. Zamawiający zastrzega termin 30.06.2025-20.07.2025 w którym szkolenia nie mogą być prowadzone.



Fundusze Europejskie
na Rozwój Cyfrowy

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA