Piano nazionale di ripresa e resilienza, Missione 4 – Istruzione e ricerca – Componente 1 – Potenziamento dell'offerta dei servizi di istruzione: dagli asili nido alle università – Investimento 3.2 "Scuola 4.0. Scuole innovative, cablaggio, nuovi ambienti di apprendimento e laboratori", finanziato dall'Unione europea – Next Generation EU – "Azione 2: Next generation labs - Laboratori per le professioni digitali del futuro".
CODICE PROGETTO: - M4C1I3.2-2022-962-P-25043
C.U.P. E34D23000600006
CIG: A02B3E69D0

CAPITOLATO TECNICO DI FORNITURA

Si intende realizzare dei Laboratori localizzati su 2 plessi, uno a Modugno e uno a Grumo Appula, tra loro interconnessi mediante VPN dedicata site-to-site con l'obiettivo di realizzare un ambiente di simulazione con scopi didattici per le seguenti attività:

- Cyber security
- Big Data
- Block Chain

A tale scopo intende dotarsi di strumentazione ed idonea infrastruttura, atta a supportare per ogni plesso un minimo 50 utenza contemporanee, in particolare:

Il plesso di Modugno dovrà essere interessato anche nella fornitura e posa in opera di nuove tratte in fibra ottica che collegheranno i laboratori posti alle estremità di ogni piano: piano terra, primo piano, secondo piano. Le nuove tratte dovranno essere posate in cavedi e canaline esistenti e saranno attestate nei rack di laboratorio.

Gli ambiente di simulazione da realizzare dovranno essere logicamente separati dalle LAN dei laboratori esistenti, segmentando la rete dei laboratori.

L'ambiente fisico deve essere virtualizzato (preferibilmente vmware vsphere).

L'intero sistema per l'ambiente di simulazione, sarà composto:

- nella Sala Server allocata nel plesso di Modugno nel laboratorio al primo piano (Turing), si avrà un Rack UPS con all'interno un Server Fisico, uno Firewall di nuova generazione Secure Firewall, uno Switch 48 GE Managed, un Access Point Wireless 1488 Mbit/s.

- Nel secondo laboratorio nella sede di Modugno (Von Neumann) posto al secondo piano, si avrà uno Switch 48 GE Managed, un Access Point Wireless 1488 Mbit/s.

- Nel laboratorio del plesso di Grumo Appula, dovrà a sua volta essere installato un rack con adeguato ups contenente uno Firewall di nuova generazione Secure Firewall, uno Switch 48 GE Managed, un Access Point Wireless 1488 Mbit/s.

Come già accennato in precedenza, i due plessi (Modugno e Grumo) devono essere collegati tramite una VPN site-to-site per garantire l'operatività, inoltre è richiesto un software di gestione degli apparati di rete, a solo titolo esemplificato:

- Umbrella Cloud Security Subscription for Education
- Umbrella DNS Security for Education

Gli ambientI di laboratorio, come precedentemente evidenziato, devono essere virtualizzati al fine di poter implementare vari ambienti di simulazione non intendendo fare sperimentazione su specifici prodotti e facendo riferimento a soluzione software open facilmente individuabili sul web (tipo github), dove sarà possibile operare su strutture già implementate e funzionanti.

Le specifiche tecniche delle apparecchiature da acquistare, con le relative quantità, sono qui di seguito elencate:

Descrizione	Quantità
Fornitura e posa in opera di dorsale fibra ottica completa di tubazione rigida e di raccorderia con collegamento sui Patch Panel;	**06**
Licenza x 03 Host per piattaforma di virtualizzazione che consente agli utenti di virtualizzare le applicazioni con scalabilità verticale e orizzontale in assoluta sicurezza attraverso un'infrastruttura on demand, flessibile e altamente disponibile (tipo VMware vSphere)	**01**
Armadio Rack da parate 9U 19" Completo (Patch Panel 48p, Passacavi, Multipresa);	**02**
Armadio Rack da pavimento 22U 19" Completo di accessori quali Patch Panel 48p, Passacavi, Multipresa e comprensivo di console KVM;	**01**
Gruppo di continuità UPS da rack 800VA (900W) TOWER/RACK-2U 2 BATTERIE USB/RS232/EPO 8XIEC SLOT SNMP	**02**
Gruppo di continuità UPS da rack 2000VA (1350W) Tower/Rack-2U 3 batterie USB/RS232/EPO 8xIEC Slot SNMP;	**01**
Server Fisico cosi configurato :	**01**

<table>
<tr><td>2 CPU INTEL XEON SILVER 4210R 128gb RAM 2 DISCHI SSD 480gb 4 PORTE 1 GbE GPU NVIDIA TESLA A40 Sistema Operativo WINDOWS SERVER 2019</td><td></td></tr>
<tr><td>Firewall di nuova generazione Secure Firewall: con software FTD, 8 porte Gigabit Ethernet (GbE), velocità di trasmissione fino a 650 Mbps
con le seguenti caratteristiche:
<table>
<tr><td>Throughput: Firewall (FW) + Application Visibility and Control (AVC) (1024B)</td><td>890 Mbps</td></tr>
<tr><td>Throughput: FW + AVC + Intrusion Prevention System (IPS) (1024B)</td><td>880 Mbps</td></tr>
<tr><td>Maximum concurrent sessions, with AVC</td><td>100K</td></tr>
<tr><td>Maximum new connections per second, with AVC</td><td>6K</td></tr>
<tr><td>Transport Layer Security (TLS)</td><td>195 Mbps</td></tr>
<tr><td>Throughput: IPS (1024B)</td><td>900 Mbps</td></tr>
<tr><td>IPSec VPN throughput (1024B TCP w/Fastpath)</td><td>400 Mbps</td></tr>
<tr><td>Maximum VPN Peers</td><td>75</td></tr>
<tr><td>Cisco Device Manager (local management)</td><td>Yes</td></tr>
<tr><td>Centralized management</td><td>Centralized configuration, logging, monitoring, and reporting are performed by the Threat Defense Manager (FMC) or, alternatively, from the cloud with Cisco Defense Orchestrator</td></tr>
<tr><td>AVC</td><td>Standard, supporting more than 4000 applications, as well as geolocations, users, and websites</td></tr>
<tr><td>AVC: OpenAppID support for custom, open-source application detectors</td><td>Standard</td></tr>
<tr><td>Cisco Security Intelligence</td><td>Standard, with IP, URL, and DNS threat intelligence</td></tr>
<tr><td>Cisco IPS</td><td>Available; can passively detect endpoints and infrastructure for threat correlation and Indicators of Compromise (IoC) intelligence</td></tr>
<tr><td>Malware Defense for Networks</td><td>Available; enables detection, blocking, tracking, analysis, and containment of targeted and persistent malware, addressing the attack continuum both during and after attacks.
Integrated threat correlation with Cisco AMP for Endpoints is also optionally available</td></tr>
<tr><td>Malware Analytics sandboxing</td><td>Available</td></tr>
</table>
</td><td><b>02</b></td></tr>
</table>

URL filtering: number of categories	More than 80
URL filtering: number of URLs categorized	More than 280 million
Automated threat feed and IPS signature updates	Yes
Third-party and open- source ecosystem	Open API for integrations with third-party products; Snort® and OpenAppID community resources for new and specific threats
High availability and clustering	Active/standby

Switch 48P Managed Switch | 48 porte GE | PoE | 4x1G SFP completo di modulo SFP e pigtail;
con le seguenti caratteristiche:

04

Capacity in Millions of Packets per Second (mpps) (64-byte packets)	77.38
Switching Capacity in Gigabits per Second (Gbps)	104.0
Spanning Tree Protocol	Standard 802.1d Spanning Tree support Fast convergence using 802.1w (Rapid Spanning Tree [RSTP]), enabled by default Multiple Spanning Tree instances using 802.1s (MSTP); 8 instances are supported Per-VLAN Spanning Tree Plus (PVST+) and Rapid PVST+ (RPVST+); 126 instances are supported
Port grouping/link aggregation	Support for IEEE 802.3ad Link Aggregation Control Protocol (LACP) ● Up to 8 groups ● Up to 8 ports per group with 16 candidate ports for each (dynamic) 802.3ad link aggregation
VLAN	Support for up to 4,094 VLANs simultaneously

	Port-based and 802.1Q tag-based VLANs; MAC-based VLAN; protocol-based VLAN; IP subnet-based VLAN Management VLAN Private VLAN with promiscuous, isolated, and community port Private VLAN Edge (PVE), also known as protected ports, with multiple uplinks Guest VLAN, unauthenticated VLAN Dynamic VLAN assignment via RADIUS server along with 802.1x client authentication CPE VLAN
Voice VLAN	Voice traffic is automatically assigned to a voice-specific VLAN and treated with appropriate levels of QoS. Voice Services Discovery Protocol (VSDP) delivers network wide zero-touch deployment of voice endpoints and call control devices
Multicast TV VLAN	Multicast TV VLAN allows the single multicast VLAN to be shared in the network while subscribers remain in separate VLANs. This feature is also known as Multicast VLAN Registration (MVR)
VLAN Translation	Support for VLAN One-to-One Mapping. In VLAN One-to-One Mapping, on an edge interface customer VLANs (C-VLANs) are mapped to service provider VLANs (S-VLANs) and the original C-VLAN tags are replaced by the specified S-VLAN
Q-in-Q	VLANs transparently cross a service provider network while isolating traffic among customers
Selective Q-in-Q	Selective Q-in-Q is an enhancement to the basic Q-in-Q feature and provides, per edge interface, multiple mappings of different C-VLANs to separate S-VLANs

	Selective Q-in-Q also allows configuring of Ethertype (Tag Protocol Identifier [TPID]) of the S-VLAN tag Layer 2 protocol tunneling over Q-in-Q is also supported
Generic VLAN Registration Protocol (GVRP)/Generic Attribute Registration Protocol (GARP)	Generic VLAN Registration Protocol (GVRP) and Generic Attribute Registration Protocol (GARP) enable automatic propagation and configuration of VLANs in a bridged domain
Unidirectional Link Detection (UDLD)	UDLD monitors physical connection to detect unidirectional links caused by incorrect wiring or cable/port faults to prevent forwarding loops and black holing of traffic in switched networks
Dynamic Host Configuration Protocol (DHCP) Relay at Layer 2	Relay of DHCP traffic to DHCP server in different VLAN; works with DHCP Option 82
Internet Group Management Protocol (IGMP) versions 1, 2, and 3 snooping	IGMP limits bandwidth-intensive multicast traffic to only the requesters; supports 2K multicast groups (source-specific multicasting is also supported)
IGMP Querier	IGMP querier is used to support a Layer 2 multicast domain of snooping switches in the absence of a multicast router
IGMP proxy	The IGMP proxy provides a mechanism for multicast forwarding based on IGMP membership information without the need for more complicated multicast routing protocols.
Head-of-Line (HOL) blocking	HOL blocking prevention
Loopback Detection	Loopback detection provides protection against loops by transmitting loop protocol packets out of ports on which loop protection has been enabled. It operates independently of STP

Layer 3	
IPv4 routing	Wirespeed routing of IPv4 packets Up to 990 static routes and up to 128 IP interfaces
IPv6 routing	Wirespeed routing of IPv6 packets
Layer 3 Interface	Configuration of Layer 3 interface on physical port, Link Aggregation (LAG), VLAN interface, or loopback interface
Classless Interdomain Routing (CIDR)	Support for classless interdomain routing
RIP v2	Support for Routing Information Protocol version 2 for dynamic routing
Policy-Based Routing (PBR)	Flexible routing control to direct packets to different next hop based on IPv4 or IPv6 Access Control List (ACL)
DHCP Server	Switch functions as an IPv4 DHCP server serving IP addresses for multiple DHCP pools/scopes Support for DHCP options
DHCP relay at Layer 3	Relay of DHCP traffic across IP domains
User Datagram Protocol (UDP) relay	Relay of broadcast information across Layer 3 domains for application discovery or relaying of Bootstrap Protocol (BOOTP)/DHCP packets
Stacking	
Hardware stacking	Up to 4 units in a stack. Up to 200 ports managed as a single system with hardware failover Stacking is supported on the following models

	CBS350-24T-4X, CBS350-24P-4X, CBS350-24FP-4X, CBS350-48T-4X, CBS350-48P-4X, CBS350-48FP-4X CBS350-8MP-2X, CBS350-24MGP-4X, CBS350-12NP-4X, CBS350-24NGP-4X, CBS350-48NGP-4X CBS350-8XT, CBS350-12XS, CBS350-12XT, CBS350-16XTS, CBS350-24XS, CBS350-24XT, CBS350-24XTS, CBS350-48XT-4X
High availability	Fast stack failover delivers minimal traffic loss. Support link aggregation across multiple units in a stack
Plug-and-play stacking configuration/management	Active/standby for resilient stack control Autonumbering Hot swap of units in stack Ring and chain stacking options, auto stacking port speed, flexible stacking port options
High-speed stack interconnects	Cost-effective high-speed 10G fiber interfaces.
Security	
Secure Shell (SSH) Protocol	SSH is a secure replacement for Telnet traffic. Secure Copy Protocol (SCP) also uses SSH. SSH v1 and v2 are supported
Secure Sockets Layer (SSL)	SSL support: Encrypts all HTTPS traffic, allowing highly secure access to the browser-based management GUI in the switch
IEEE 802.1X (Authenticator role)	802.1X: Remote Authentication Dial-In User Service (RADIUS) authentication and accounting, MD5 hash; guest VLAN; unauthenticated VLAN, single/multiple host mode and single/multiple sessions Supports time-based 802.1X; dynamic VLAN assignment; MAC authentication

IEEE 802.1X supplicant	A switch can be configured to act as a supplicant to another switch. This enables extended secure access in areas outside the wiring closet (such as conference rooms)
Web-based authentication	Web-based authentication provides network admission control through web browser to any host devices and operating systems
STP Bridge Protocol Data Unit (BPDU) Guard	A security mechanism to protect the network from invalid configurations. A port enabled for BPDU Guard is shut down if a BPDU message is received on that port. This avoids accidental topology loops
STP Root Guard	This prevents edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes
STP loopback guard	Provides additional protection against Layer 2 forwarding loops (STP loops)
DHCP snooping	Filters out DHCP messages with unregistered IP addresses and/or from unexpected or untrusted interfaces. This prevents rogue devices from behaving as DHCP Servers.
IP Source Guard (IPSG)	When IP Source Guard is enabled at a port, the switch filters out IP packets received from the port if the source IP addresses of the packets have not been statically configured or dynamically learned from DHCP snooping. This prevents IP address spoofing.
Dynamic ARP Inspection (DAI)	The switch discards ARP packets from a port if there are no static or dynamic IP/MAC bindings or if there is a discrepancy between the source or

	destination addresses in the ARP packet. This prevents man-in-the-middle attacks.
IP/MAC/Port Binding (IPMB)	The preceding features (DHCP Snooping, IP Source Guard, and Dynamic ARP Inspection) work together to prevent DOS attacks in the network, thereby increasing network availability
Secure Core Technology (SCT)	Makes sure that the switch will receive and process management and protocol traffic no matter how much traffic is received
Secure Sensitive Data (SSD)	A mechanism to manage sensitive data (such as passwords, keys, and so on) securely on the switch, populating this data to other devices, and secure autoconfig. Access to view the sensitive data as plaintext or encrypted is provided according to the user-configured access level and the access method of the user.
Trustworthy systems	Trustworthy systems provide a highly secure foundation for Cisco products Run-time defenses (Executable Space Protection [X-Space], Address Space Layout Randomization [ASLR], Built-In Object Size Checking [BOSC])
Private VLAN	Private VLAN provides security and isolation between switch ports, which helps ensure that users cannot snoop on other users' traffic; supports multiple uplinks
Layer 2 isolation Private VLAN Edge (PVE)	PVE (also known as protected ports) provides Layer 2 isolation between devices in the same VLAN, supports multiple uplinks
Port security	Ability to lock source MAC addresses to ports and limits the number of learned MAC addresses

RADIUS/TACACS+	Supports RADIUS and TACACS authentication. Switch functions as a client
RADIUS accounting	The RADIUS accounting functions allow data to be sent at the start and end of services, indicating the amount of resources (such as time, packets, bytes, and so on) used during the session
Storm control	Broadcast, multicast, and unknown unicast
DoS prevention	Denial-of-Service (DOS) attack prevention
Multiple user privilege levels in CLI	Level 1, 7, and 15 privilege levels
ACLs	Support for up to 1,024 rules Drop or rate limit based on source and destination MAC, VLAN ID, IPv4 or IPv6 address, IPv6 flow label, protocol, port, Differentiated Services Code Point (DSCP)/IP precedence, Transmission Control Protocol/User Datagram Protocol (TCP/UDP) source and destination ports, 802.1p priority, Ethernet type, Internet Control Message Protocol (ICMP) packets, IGMP packets, TCP flag; ACL can be applied on both ingress and egress sides Time-based ACLs supported

Access Point wireless access point 1488 Mbit/s Power over Ethernet [PoE]
con le seguenti caratteristiche:

04

802.11n version 2.0 (and related) capabilities	● 2x2 MIMO with two spatial streams ● Maximal Ratio Combining (MRC) ● 802.11n and 802.11a/g ● 20- and 40-MHz channels

	● PHY data rates up to 444.4 Mbps (40 MHz with 5 GHz and 20 MHz with 2.4 GHz) ● Packet aggregation: Aggregate MAC Protocol Data Unit (A-MPDU) (transmit and receive), Aggregate MAC Service Data Unit (A-MSDU) (transmit and receive) ● 802.11 Dynamic Frequency Selection (DFS) ● Cyclic Shift Diversity (CSD) support	
802.11ac	● 2x2 downlink MU-MIMO with two spatial streams ● MRC ● 802.11ac beamforming ● 20-, 40-, 80- MHz channels ● PHY data rates up to 866.7 Mbps (80 MHz with 5GHz) ● Packet aggregation: A-MPDU (transmit and receive), A-MSDU (transmit and receive) ● 802.11 DFS ● CSD support ● WPA3 support	
802.11ax	● 2x2 uplink/downlink MU-MIMO with two spatial streams ● Uplink/downlink OFDMA ● TWT ● BSS coloring ● MRC ● 802.11ax beamforming ● 20-, 40-, 80- channels ● PHY data rates up to 1.488 Gbps (80 MHz with 5 GHz and 20 MHz with 2.4 GHz) ● Packet aggregation: A-MPDU (transmit and receive), A-MSDU (transmit and receive) ● 802.11 DFS ● CSD support ● WPA3 support	
Integrated antenna	● 2.4 GHz: Peak gain 4 dBi, internal antenna, omnidirectional in azimuth ● 5 GHz: Peak gain 5 dBi, internal antenna, omnidirectional in azimuth	
Interfaces	● 1x 10/100/1000 Base-T (Ethernet) Uplink Interface ● Management console port (RJ-45)	
Indicators	● Status LED indicates boot loader status, association status, operating status, boot loader warnings, and boot loader errors	

<table>
<tr><td>
<table>
<tr><td>Dimensions
(W x L x H)</td><td colspan="4">● Access point (without mounting brackets):
5.9 x 5.9 x 1.18 in. (150 x 150 x 30 mm)</td></tr>
<tr><td>Weight</td><td colspan="4">0.7 lb. (329.5g)</td></tr>
<tr><td rowspan="4">Input power requirements</td><td colspan="4">● 802.3at Power over Ethernet Plus (PoE+), Cisco Universal PoE (Cisco UPOE)
● Cisco power injector, AIR-PWRINJ6=
● 802.3af PoE
● Cisco power injector, AIR-PWRINJ5= (Note: This injector supports only 802.3af)</td></tr>
<tr><td colspan="4">Catalyst 9105AXI</td></tr>
<tr><td>PoE power</td><td>2.4-GHz radio</td><td>5-GHz radio</td><td>Link speed</td></tr>
<tr><td>802.3af (PoE)</td><td>2x2</td><td>2x2</td><td>1G</td></tr>
<tr><td>Environmental</td><td colspan="4">● Nonoperating (storage) temperature: -22° to 158°F (-30° to 70°C)
● Nonoperating (storage) altitude test: 25℃, 15,000 ft (4600 m)
● Operating temperature: 32° to 122°F (0° to 50°C)
● Operating humidity: 10% to 90% (noncondensing)
● Operating altitude test: 40℃, 9843 ft.(3000 m)
Note: When the ambient operating temperature exceeds 40°C, the access point will shift from 2x2 to 1x1 on the 2.4 GHz radio.</td></tr>
<tr><td rowspan="2">Available transmit power settings (Max/Min)</td><td colspan="4"></td></tr>
<tr><td>● 2.4 GHz
◦ 20 dBm (100 mW)
◦ -7 dBm (0.2 mW)</td><td>● 5 GHz
◦ 20 dBm (100 mW)
◦ -7 dBm (0.2 mW)</td></tr>
</table>
</td><td></td></tr>
<tr><td>Modulo Transceiver SFP-SX Gigabit Multimodale, connettore LC</td><td>02</td></tr>
</table>

Tutta la Strumentazione sopra descritta sarà configurata in modo tale da implementare i vari ambiente di simulazione con scopi didattici descritti all'inizio di questo documento

Ogni singolo Ambiente di apprendimento saranno dotati di software necessari alla implementazione degli scopi didattici per i quale l'ambiente di apprendimento è stato creato.

Per ogni ambiente e per ogni software è prevista l'installazione, la configurazione e l'addestramento:

Si dettagliano, qui si seguito, per ogni singolo ambiente i software richiesti.

Ambiente di CYBER SECURITY

- **Vulnerability Assessment**
  OpenVAS - Sistema di scansione di vulnerabilità per reti e applicazioni che supporta diverse lingue e offre un'ampia gamma di funzionalità per la scansione dei sistemi.

- **Penetration Test**
  Metasploit - Piattaforma di test di penetrazione utilizzata per simulare attacchi e testare la sicurezza dei sistemi informatici.

- **WebSecurity**
  OWASP ZAP - Strumento di test di sicurezza delle applicazioni Web che offre una vasta gamma di funzionalità, tra cui la scansione e il testing.

Ambiente di BIG DATA

- **Apache Hadoop** - Un framework popolare per lo storage distribuito e l'elaborazione di grandi set di dati.
- **Apache Spark** - Un sistema di calcolo cluster veloce e generale per l'elaborazione di big data.
- **Apache Flink** - Un motore di elaborazione di dati in streaming per l'analisi in tempo reale.
- **Apache Storm** - Un sistema di elaborazione di calcolo distribuito in tempo reale per l'elaborazione di flussi di dati.
- **Apache Cassandra** - Un database NoSQL distribuito per la gestione di grandi quantità di dati.

Ambiente BLOCKCHAIN

- **Hyperledger Composer**: è uno strumento di sviluppo open source per creare applicazioni blockchain. Utilizza un'interfaccia grafica utente per semplificare il processo di creazione di smart contract e la gestione della blockchain. Hyperledger Composer è basato su Hyperledger Fabric, un framework di blockchain aziendale open source.

- **Ethereum Studio**: è un ambiente di sviluppo integrato (IDE) che permette di creare, testare e distribuire applicazioni basate sulla blockchain Ethereum. Utilizza un'interfaccia utente intuitiva e semplifica il processo di sviluppo di smart contract.
- **Ganache:** è un ambiente di sviluppo locale per la blockchain Ethereum. Consente di eseguire una blockchain Ethereum locale e di testare gli smart contract senza dover effettuare transazioni reali sulla blockchain principale.
- **Remix:** è un IDE per la creazione di smart contract sulla blockchain Ethereum. Offre un'interfaccia utente semplice e intuitiva, e consente di creare, testare e distribuire smart contract sulla blockchain.
- **Truffle**: è uno strumento di sviluppo per la blockchain Ethereum. Consente di creare, testare e distribuire smart contract sulla blockchain e semplifica il processo di sviluppo.

Per tutti gli ambienti, gli apparati, le strumentazioni, gli applicativi forniti e sopracitati si richiede l'installazione, la configurazione ed addestramento.

Firmato digitalmente da:
GIANNETTO ROSARIA
Firmato il 22/11/2023 09:13
Seriale Certificato: 1827254
Valido dal 12/10/2022 al 12/10/2025
InfoCamere Qualified Electronic Signature CA