Allegato n. 1

SCHEDA 1:

Parte 1: Problem Solving su Architetture Web a Tre Livelli (WAF - Firewall - FE/BE)

Scenario Architetturale: Un'applicazione web di Ateneo (Verbalizzazione Esami) è strutturata con un WAF perimetrale come Reverse Proxy, un Firewall di frontiera, un pool di server di Front-End (DMZ) e un cluster Database di Back-End in una subnet interna protetta.
Il Problema: Gli studenti segnalano che, provando a salvare i dati di un esame, il portale restituisce un errore generico **HTTP 502 Bad Gateway** o **HTTP 504 Gateway Timeout.** Lato WAF i log non mostrano violazioni di sicurezza (no attacchi bloccati), ma il servizio è di fatto inutilizzabile.
Domanda: Descrivi l'approccio analitico e la catena di verifiche tecniche (comandi, log e stati degli apparati) che adotteresti per isolare il guasto, specificando come determini se il blocco risiede nella comunicazione tra WAF e Front-End, tra Front-End e Firewall interno, o se si tratta di un drop di sessione o saturazione delle connessioni sul Database di Back-End.

Parte 2: Progettazione su Routing BGP e Infrastruttura Data Center L2 (MC-LAG)

- **L'Esigenza:** L'Ateneo deve interconnettere il proprio Data Center principale a un nuovo anello in fibra ottica metropolitano (fornito da un consorzio di ricerca) mantenendo attiva, in modalità failover, la preesistente connettività internet commerciale. La rete interna del Data Center deve garantire la massima ridondanza a livello 2 per evitare che il guasto di un singolo switch di distribuzione isoli interi segmenti di server.
- **Domanda :** Disegna e descrivi lo scenario architetturale ottimale per soddisfare questa esigenza. Specifica come configureresti le sessioni di routing verso l'esterno e quale tecnologia di aggregazione e multihoming adotteresti a livello core/distribution per garantire la resilienza L2, dettagliando il posizionamento dei Default Gateway.

Parte 3: Comprensione della Lingua Inglese Tecnica (Topic: Fundamentals of Identity and Access Management - IAM)

Technical Text: "Identity and Access Management (IAM) is a core framework of policies and technologies designed to ensure that the right individuals have access to the right technology resources at the right time. Modern IAM solutions operate on two fundamental security principles: Role-Based Access Control (RBAC) and the Principle of Least Privilege. RBAC simplifies administration by assigning permissions to specific organizational roles rather than individual users. The Principle of Least Privilege dictates that users must only be granted the minimum level of access necessary to complete their job functions. By implementing centralized Single Sign-On

(SSO), enterprises can enforce these access policies consistently across both legacy local systems and hybrid cloud services, drastically reducing the organization's overall attack surface."

- **Domanda :** Il candidato riassuma i due concetti chiave di sicurezza (RBAC e *Least Privilege*) descritti nel testo e spieghi in che modo la centralizzazione tramite Single Sign-On (SSO) contribuisce a migliorare la sicurezza e la gestione dei sistemi.

SCHEDA 2:

Parte 1: Problem Solving su Routing BGP e Infrastruttura L2 in MC-LAG

Scenario Architetturale: L'Ateneo è attestato sulla rete Internet tramite un unico Router di frontiera che gestisce il routing dinamico tramite sessioni BGP (eBGP verso il provider esterno). Verso la rete interna del Data Center, il Router è interconnesso alla fabric tramite un doppio link fisico configurato in aggregazione logica (LACP/Port-Channel). Per garantire l'alta affidabilità a Livello 2, questo doppio link è attestato in modalità multihoming su due switch distinti della fabric, configurati in MC-LAG (Multi-Chassis Link Aggregation). Le diverse VLAN dei servizi dell'Ateneo transitano in modalità trunk su questo bundle logico.

Il Problema: A seguito di un micro-blackout in sala macchine e del conseguente riavvio di uno dei due switch che compongono il cluster MC-LAG, si nota che la sessione eBGP sul router si è correttamente riattivata e il traffico verso l'esterno converge. Tuttavia, alcuni servizi critici attestati su specifiche VLAN interne risultano parzialmente o totalmente irraggiungibili dall'esterno, evidenziando un forte drop di pacchetti o problemi di instradamento intermittenti.

Domanda: Descrivi la metodologia di isolamento del guasto a Livello 2 e Livello 3. Quali verifiche analitiche effettueresti sulle tabelle e sullo stato dell'MC-LAG (Peer-Link, Keepalive) e sulla consistenza del protocollo LACP del doppio link attestato sul router? Come verifichi, lato Livello 3, che le tabelle di routing BGP e le adiacenze non risentano di anomalie di inoltro causate dal disallineamento della sottostante topologia di Livello 2?

Parte 2: Progettazione su Reti Wireless Enterprise Cloud-Managed (Radius/802.1X)

- **L'Esigenza:** L'Ateneo deve implementare la copertura Wi-Fi in un intero polo didattico distaccato di nuova acquisizione. L'amministrazione richiede una soluzione agile, priva di hardware di controllo (WLC) locale on-premise, che permetta una gestione centralizzata basata su policy e garantisca l'accesso sicuro a studenti e docenti tramite le credenziali istituzionali centrali già in uso.
- **Domanda:** Proponi il design architetturale ottimale per questa infrastruttura wireless. Descrivi come si articola l'interazione tra gli apparati periferici, la piattaforma di management e i sistemi di autenticazione centralizzati dell'Ateneo, specificando i protocolli coinvolti sia per il piano di controllo sia per il piano di dati.

Parte 3: Comprensione della Lingua Inglese Tecnica (Topic: Fundamentals of Identity and Access Management - IAM)

Technical Text: "Identity and Access Management (IAM) is a core framework of policies and technologies designed to ensure that the right individuals have access to the right technology resources at the right time. Modern IAM solutions operate on two fundamental security principles: Role-Based Access Control (RBAC) and the Principle of Least Privilege. RBAC simplifies administration by

assigning permissions to specific organizational roles rather than individual users. The Principle of Least Privilege dictates that users must only be granted the minimum level of access necessary to complete their job functions. By implementing centralized Single Sign-On (SSO), enterprises can enforce these access policies consistently across both legacy local systems and hybrid cloud services, drastically reducing the organization's overall attack surface."

- **Domanda:** Riassuma i due concetti chiave di sicurezza (RBAC e *Least Privilege*) descritti nel testo e spieghi in che modo la centralizzazione tramite Single Sign-On (SSO) contribuisce a migliorare la sicurezza e la gestione dei sistemi.

SCHEDA 3:

Parte 1: Problem Solving su Reti Wireless Enterprise Gestite in Cloud (Cloud-Managed AP - Radius/802.1X)

Scenario Architetturale

La rete Wi-Fi dell'Ateneo (SSID unico) adotta un'**architettura cloud-managed** (es. Cisco Meraki, Aruba Central o CommScope RUCKUS One), priva di un Wireless LAN Controller (WLC) fisico on-premise. Gli Access Point (AP) dislocati nei plessi scaricano la configurazione e inviano la telemetria direttamente alla Dashboard in Cloud tramite connessione Internet protetta. Il traffico dati degli utenti viene terminato (bridged) localmente sulle VLAN della rete cablata d'Ateneo, mentre l'autenticazione enterprise (802.1X) viene demandata dagli AP direttamente a un server RADIUS locale (es. Cisco ISE o FreeRADIUS).

Il Problema: Durante una sessione di esami scritti al computer in un'aula magna, cinquanta studenti contemporaneamente lamentano l'impossibilità di connettersi: i loro dispositivi rimangono bloccati sulla fase di "Identificazione in corso..." o restituiscono un errore di "Impossibile connettersi a questa rete". Dalla Dashboard Cloud, gli AP dell'aula risultano "Online" e correttamente raggiungibili.

Domanda: Spiega come analizzi analiticamente il problema per isolare la causa radice sfruttando gli strumenti della Dashboard Cloud e dell'infrastruttura locale. In che modo determini se il problema è causato da un mancato transito del traffico RADIUS (802.1X) tra gli AP e il server di autenticazione, da un esaurimento del pool DHCP sulla VLAN locale dell'aula, o da un problema di connettività degli AP verso i servizi cloud?

Parte 2: Progettazione su Infrastrutture Cloud Ibrido (Identity & Access Management)

- **L'Esigenza:** L'Ateneo deve estendere il proprio sistema di identità locale, basato su Active Directory Domain Services (AD DS), verso il cloud Microsoft Azure/Entra ID per abilitare l'ecosistema Microsoft 365 per 30.000 studenti e 4.000 dipendenti. I requisiti fondamentali sono l'adozione del Single Sign-On (SSO), la non-replicazione delle password in chiaro sul cloud e l'applicazione di policy di Multi-Factor Authentication (MFA) contestuali (es. in base alla geolocalizzazione o al tipo di dispositivo).
- **Domanda 2:** Disegna l'architettura logica e infrastrutturale di questa soluzione ibrida. Specifica quali componenti software e agenti locali devono essere installati, come viene configurato il flusso di sincronizzazione e come viene gestito il ciclo di autenticazione dell'utente quando tenta l'accesso a Microsoft 365.

Parte 3: Comprensione della Lingua Inglese Tecnica (Topic: The Principles of Network Segmentation and DMZs)

Technical Text: "Network segmentation is an architectural approach that divides a monolithic computer network into smaller, isolated subnetworks. By breaking the network into logical zones based on function

and trust levels, organizations can tightly control the flow of traffic using firewalls and access control lists. A classic implementation of this strategy is the Demilitarized Zone (DMZ), an isolated subnet that acts as a buffer between the untrusted public Internet and the highly secure internal corporate network. External-facing services, such as public web servers, are placed inside the DMZ. If an attacker compromises a server located in the DMZ, the strict firewall rules applied to the internal perimeter prevent the threat from moving laterally into the core backend databases."

- **Domanda:** Qual è lo scopo fondamentale della segmentazione di rete secondo il testo e quale ruolo strategico riveste la *Demilitarized Zone* (DMZ) nel contrasto ai movimenti laterali di un utente malintenzionato?

SCHEDA 4:

Parte1: Problem Solving su Cloud Ibrido (On-Premise - Microsoft Entra ID / Office 365)

Scenario Architetturale: L'Ateneo adotta un modello cloud ibrido: la gestione delle identità risiede su Active Directory Domain Services (AD DS) on-premise, sincronizzato tramite Microsoft Entra Connect verso il cloud per l'accesso ai servizi Office 365 (Exchange Online, Teams) tramite Single Sign-On (SSO).
Il Problema: Subito dopo un intervento di manutenzione sui domain controller locali, numerosi docenti segnalano che riescono ad accedere regolarmente ai PC dell'ufficio e alla intranet locale, ma non riescono più ad accedere alla posta di Office 365 dal browser, ricevendo un errore di autenticazione o di mancata sincronizzazione dell'account.
Domanda: Qual è il tuo flusso logico di troubleshooting sistemistico? Quali verifiche effettueresti sul server Microsoft Entra Connect (log di sincronizzazione, agenti di pass-through authentication) e quali strumenti o cmdlet di PowerShell utilizzeresti per diagnosticare se il guasto dipende da un blocco delle porte di rete outbound verso il cloud o da un disallineamento degli attributi immutabili (es. ObjectGUID / sourceAnchor) degli utenti?

PARTE 2: Progettazione su Identity Provider e Accesso VPN Sicuro (Firewall - Gateway VPN - AD)

- **L'Esigenza:** L'Ateneo deve implementare una nuova infrastruttura di accesso remoto sicuro (VPN) destinata al personale tecnico-amministrativo e ai fornitori esterni per la manutenzione dei sistemi core. La soluzione deve garantire la granularità degli accessi (gli utenti devono accedere solo alle risorse di propria competenza), l'integrazione con l'Identity Provider (IdP) centralizzato di Ateneo e canali trasmissivi fortemente cifrati.
- **Domanda:** Sviluppa il progetto di questa architettura di sicurezza. Descrivi la tipologia di VPN scelta, le modalità di cifratura, i protocolli di comunicazione tra il Gateway VPN e l'IdP/Active Directory per la mappatura dei profili utente, e i meccanismi di protezione perimetrale applicati alle sessioni VPN.

Parte 3: Comprensione della Lingua Inglese Tecnica (Topic: The NIS Directive and Cyber Resilience)

Technical Text: "The Network and Information Security (NIS) Directive establishes a comprehensive legal framework aimed at increasing the baseline level of cybersecurity and cyber resilience across critical sectors. Under this European regulation, public administrations, educational entities, and essential service operators are required to adopt robust risk-management measures and technical controls to safeguard their network infrastructure. A fundamental component of compliance involves structural accountability: organizations must maintain continuous visibility over their assets, implement active incident-detection

mechanisms, and adhere to strict mandatory reporting timelines to notify national authorities of significant security breaches. Ultimately, the goal is to shift security from a reactive model to a proactive posture of continuous monitoring."

Domanda: Quali sono gli obblighi principali normativi e tecnici che la Direttiva NIS impone alle amministrazioni pubbliche e agli enti di istruzione per garantire la cyber resilience e la corretta gestione degli incidenti informatici?

SCHEDA 5:

Parte 1: Problem Solving su Identity Provider e Accesso VPN (Firewall - VPN Gateway - AD/LDAP)

Scenario Architetturale: Il personale tecnico accede alle risorse critiche da remoto tramite un gateway VPN SSL attestato sul Firewall perimetrale. Il Firewall agisce come client di un Identity Provider (IdP) interno centralizzato, che convalida le credenziali e l'appartenenza ai gruppi di sicurezza tramite interrogazioni LDAP/LDAPS su Active Directory locale.
Il Problema: A seguito dell'aggiornamento dei certificati di sicurezza sui Domain Controller, tutti gli utenti VPN che tentano il login ricevono il messaggio "Credenziali non valide", bloccando l'assistenza remota. Dai controlli interni, gli stessi utenti si autenticano senza problemi sui servizi locali in ufficio.
Domanda: Analizza la catena di autenticazione. Come utilizzi i log del Firewall/VPN Gateway per capire dove si interrompe il processo? Quali verifiche effettui sulla configurazione del connettore LDAP del firewall, con particolare riferimento alla porta utilizzata (636 vs 389), alla validità della CA del certificato importato e alla cifratura del canale, per risolvere il disservizio?

Parte 2: Progettazione su Storage, Virtualizzazione e Network Convergente (vSAN e vDS)

- **L'Esigenza:** Nell'ambito del consolidamento dei propri servizi d'Ateneo, si richiede la progettazione di un nuovo cluster di virtualizzazione ad alta affidabilità composto da 4 nodi computazionali x86. Al fine di ridurre i costi di gestione e superare i limiti delle tradizionali SAN architettate su switch Fibre Channel, si opta per una soluzione di storage iperconvergente integrata nell'hypervisor, garantendo elevate performance di I/O e la totale ridondanza logica e fisica della rete.
- **Domanda:** Elabora il design di questa infrastruttura iperconvergente basata su tecnologia **VMware vSAN** e **vSphere Distributed Switch (vDS)**. Descrivi i requisiti hardware minimi dei nodi, la configurazione logica dei distributed port groups e l'architettura della rete fisica (Core/Leaf) necessaria a supportare il traffico storage e computazionale a bassissima latenza.

Parte 3: Comprensione della Lingua Inglese Tecnica (Topic: Enterprise Wireless Architecture Concepts)

Technical Text: "Enterprise wireless networking demands a clear separation between the management plane, the control plane, and the data plane to handle dense client environments effectively. In traditional deployments, a hardware Wireless LAN Controller (WLC) coordinates radio frequency (RF) channels, transmit power, and roaming across all Access Points (APs). In modern cloud-managed frameworks, the control and management planes are moved to a remote software platform, while the data plane is fully decentralized. This means user data packets are

bridged directly onto the local wired switches at the edge, removing the architectural bandwidth bottlenecks associated with tunneling all traffic back to a central physical appliance."

- **Domanda:** Spieghi come viene distribuito il traffico dati (*data plane*) e quello di controllo (*control/management plane*) in una moderna architettura wireless di tipo cloud-managed rispetto a un'architettura tradizionale basata su WLC fisico.

SCHEDA 6:

Parte 1: Problem Solving su Storage, Virtualizzazione e Network Convergente (vSAN e vDS)

Scenario Architetturale: L'infrastruttura Data Center di Ateneo poggia su due cluster di virtualizzazione VMware vSphere i cui host memorizzano le macchine virtuali (VM) utilizzando uno storage enterprise di tipo **vSAN (Virtual SAN)**. La connettività di rete è interamente virtualizzata tramite **vSphere Distributed Switch (vDS)**, i quali mappano il traffico di management, vMotion e vSAN su uplink fisici ridondati connessi agli switch della rete fisica (Core/Leaf).
Il Problema: Durante un'attività di manutenzione e migrazione sulla rete fisica, una delle interfacce o dei segmenti dedicati al traffico storage subisce un'interruzione di connettività. Di conseguenza, nel vCenter alcune macchine virtuali server critiche entrano in uno stato di **"Inaccessible" o "Orphaned"**, mentre altre rimangono attive ma registrano latenze di I/O disco elevatissime, degradando o bloccando i servizi agli utenti.
Domanda: Fornisci un'analisi metodologica del guasto focalizzandoti sul rapporto tra rete virtuale e rete fisica. Come determini se il problema è legato a un disallineamento della configurazione di rete (es. MTU errata / Jumbo Frame non configurati end-to-end sui vDS o sugli switch fisici), a un problema di tagging VLAN sulle porte trunk fisiche, o a un partizionamento del cluster vSAN? Quali comandi CLI e strumenti di diagnostica utilizzeresti sugli host ESXi per verificare la mappatura della rete prima di valutare un failover sul sito di Disaster Recovery?

Parte 2: Progettazione su Architetture Web Scalabili e Sicure a Tre Livelli (WAF - FW - FE/BE)

- **L'Esigenza:** L'Ateneo deve pubblicare il nuovo "Portale Unico dello Studente", un'applicazione web critica che sperimenta carichi transitori enormi durante le finestre di immatricolazione annuale (fino a 15.000 utenti simultanei). I requisiti stringenti includono la protezione totale contro attacchi volumetrici e applicativi, la scalabilità orizzontale automatica del livello web e l'isolamento del database contenente i dati sensibili degli iscritti.
- **Domanda:** Disegna lo scenario architetturale ottimale a tre livelli per questa applicazione. Descrivi il posizionamento e le funzionalità degli apparati di sicurezza perimetrale applicativa, dei sistemi di bilanciamento del carico, del pool di Front-End e del cluster database di Back-End, dettagliando le regole di isolamento di rete (DMZ vs Subnet protette).

PARTE 3: Comprensione della Lingua Inglese Tecnica (Topic: Software-Defined Storage and Storage Virtualization)

Technical Text: "Software-Defined Storage (SDS) abstracts physical storage resources from the underlying hardware, pooling them into a single logical entity managed through software. In virtualized data centers, this approach eliminates the traditional storage silos built on proprietary

Storage Area Networks (SANs). By pooling local solid-state drives (SSDs) across multiple cluster hosts, the hypervisor can deliver low-latency shared storage directly over standard Ethernet networks. Storage policies can then be applied at a granular, per-virtual-machine level. This integration ensures that computing and storage scale together horizontally, dramatically reducing physical footprint while simplifying capacity planning and infrastructure orchestration."

- **Domanda:** Quali sono i benefici e le caratteristiche distintive dell'approccio *Software-Defined Storage* (SDS) all'interno di un data center virtualizzato rispetto all'utilizzo delle tradizionali architetture SAN fisiche?