Sezione tecnologie per l’azienda

Corso cybersecurity

Il Firewall - Prima Linea di Difesa

- Dispositivo di sicurezza di rete che monitora e filtra il traffico in entrata e in uscita
- Funzionamento base
  - Analisi basata su regole predefinite (ACL - Access Control Lists)
- Tipologie principali
  - Packet Filtering: Analisi solo dell'intestazione IP/Porta (Stateless)
  - Stateful Inspection: Traccia lo stato delle connessioni attive (contesto)
  - Next-Generation Firewall (NGFW): Ispezione profonda (DPI), controllo applicazioni e identità utente
- Posizionamento
  - Perimetro rete, tra segmenti interni, o host-based

Configurazione Firewall - Best Practices

- Principio del "Default Deny"
  - Bloccare tutto il traffico che non è esplicitamente permesso
- Regola dell'ordine (Rule Ordering)
  - Le regole più specifiche vanno in cima, quelle generiche in fondo
- Logging e Audit
  - Abilitare i log per il traffico scartato (DROP) per analisi forensi
- Gestione delle porte
  - Chiudere porte non necessarie (es Telnet 23, SSH, FTP, netbios, ...)
  - Limitare l'accesso amministrativo (SSH/RDP) solo a IP specifici o via VPN
- Revisione periodica
  - Eliminare regole obsolete (shadow rules) ogni 6 mesi

Esempio Pratico: Configurazione Regole Firewall

- Protezione di un Web Server Linux
  - Regola 1 (Inbound): Allow TCP port 443 (HTTPS) from ANY to WebServer_IP
  - Regola 2 (Inbound): Allow TCP port 22 (SSH) from Admin_VPN_Subnet to WebServer_IP
  - Regola 3 (Outbound): Allow TCP port 3306 (MySQL) from WebServer_IP to DB_Server_IP
  - Regola 4 (Outbound): Allow UDP port 53 (DNS) from WebServer_IP to DNS_Servers
  - Regola 5 (Cleanup): Deny ALL traffic from ANY to ANY (Log enabled)

Proxy Server - Intermediari di Rete

- Intermediario tra client e server che inoltra le richieste per conto del richiedente
  - Forward Proxy: Protegge i client interni che navigano su Internet (es filtraggio URL aziendale)
  - Reverse Proxy: Protegge i server aziendali dalle richieste esterne (bilanciamento del carico, offloading SSL)
  - Vantaggi di sicurezza: Nasconde l'IP reale dei server interni e ispeziona il contenuto applicativo
  - Caching: Memorizza contenuti frequenti per ridurre la latenza e il carico di rete

Differenze Operative tra Firewall e Proxy

- Livello TCP/IP
  - Firewall: Lavora sui livelli Internet e Trasporto Filtra in base a Indirizzi IP, Porte (TCP/UDP) e stato della connessione
  - Proxy: Lavora sul livello Applicazione Comprende i protocolli (HTTP, FTP, SMTP) e il contenuto dei dati
- Profondità di Analisi
  - Il Proxy "apre" il pacchetto e ne legge il contenuto (payload), il Firewall tradizionale guarda l'intestazione (header)
- Decrittazione
  - I Proxy sono essenziali per l'ispezione SSL/TLS (Man-in-the-Middle autorizzato) dove il Firewall spesso è cieco
- Interazione Utente
  - Il Proxy può chiedere autenticazione attiva (login) prima di dare accesso, il Firewall è trasparente
- Utilizzo Combinato
  - Firewall per velocità e protezione di base, Proxy per controllo contenuti e privacy

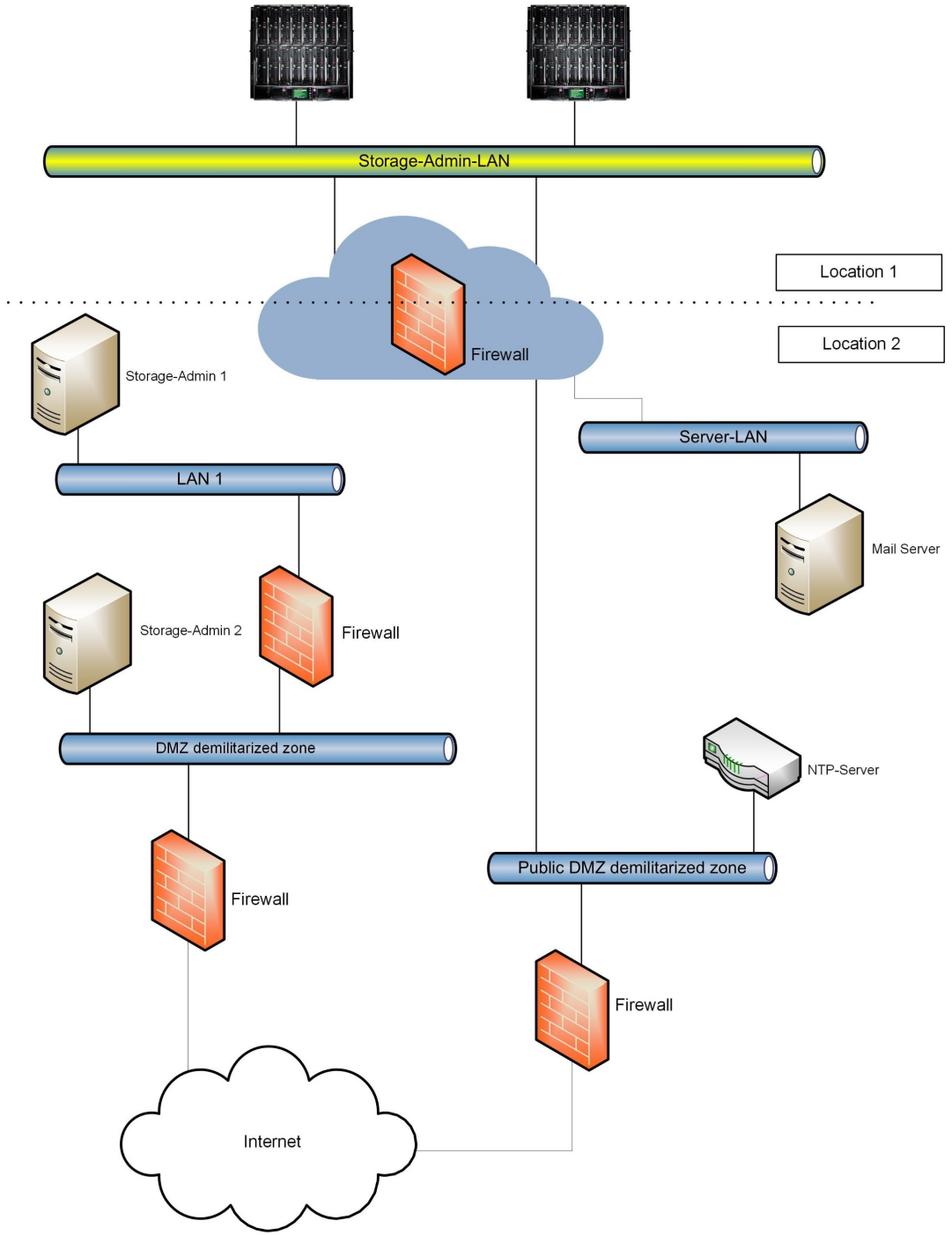
Configurazione Proxy Sicura

- Blacklist vs Whitelist
  - Bloccare categorie note (gambling, malware) o permettere solo siti approvati
- Content Filtering
  - Scansione antivirus in tempo reale sui file scaricati
- Data Loss Prevention (DLP)
  - Bloccare l'upload di file sensibili o dati aziendali verso l'esterno
- Header Sanitization
  - Rimuovere header HTTP che rivelano info interne (es versione server)
- Log Retention
  - Mantenere i log di navigazione conforme alle policy GDPR/Privacy

La DMZ (Demilitarized Zone)

- Una sottorete fisica o logica che separa la rete interna (LAN) da reti non affidabili (Internet)
- Scopo
  - Esporre i servizi pubblici (Web, Mail, DNS) senza compromettere la rete interna
- Isolamento
  - Se un server in DMZ viene compromesso, l'hacker non ha accesso diretto ai dati sensibili in LAN
- Regole di traffico
  - Internet -> DMZ: Permesso (porte specifiche)
  - DMZ -> LAN: Negato (o strettamente limitato)
  - LAN -> DMZ: Permesso (per gestione)
  - DMZ -> Internet: Permesso

La DMZ (Demilitarized Zone)



Architetture DMZ Comuni

- Single Firewall (3-Legged)
  - Un firewall con tre interfacce (WAN, LAN, DMZ) Più economico, singolo punto di fallimento
- Dual Firewall (Back-to-Back)
  - Front-end Firewall: Filtra traffico da Internet alla DMZ
  - Back-end Firewall: Filtra traffico dalla DMZ alla LAN
- Vantaggio Dual Firewall
  - Permette di usare vendor diversi per i due firewall (Security through Diversity)
- Micro-segmentazione in DMZ
  - Separare anche i server all'interno della DMZ stessa (es Web separato da Mail)

Segmentazione della Rete

- Pratica di dividere una rete in sottoreti più piccole (Subnet/VLAN)
- Obiettivo primario
  - Ridurre la superficie d'attacco e limitare il movimento laterale degli attaccanti
- Performance
  - Riduce la congestione del traffico broadcast migliorando l'efficienza
- Visibilità
  - Facilita il monitoraggio del traffico anomalo tra dipartimenti
- Compliance
  - Spesso richiesta da normative (es PCI-DSS per dati carte di credito)

Tecniche di Segmentazione

- VLAN (Virtual LAN)
  - Segmentazione logica a livello Switch Reparti diversi (HR, IT, Sales) su VLAN diverse
- Subnetting
  - Segmentazione a livello IP addressing, collegata tramite router/firewall
- Firewall Interni
  - Posizionare firewall tra segmenti critici (es tra Rete Utenti e Rete Server)
- Software-Defined Segmentation
  - Uso di tag e policy logiche indipendentemente dalla topologia fisica (modello Zero Trust)
- Air Gapping
  - Separazione fisica totale per reti ad altissima sicurezza (es sistemi SCADA/Industriali)

Esempio: Segmentazione "Zero Trust"

- Scenario: Un attaccante compromette il PC di una segretaria (VLAN Utenti)
  - Senza Segmentazione
    - L'attaccante scansiona tutta la rete e raggiunge il Server Database
  - Con Segmentazione
    - Il PC è nella VLAN 10 (Utenti)
    - Il DB è nella VLAN 50 (Server)
    - L'ACL sul firewall blocca traffico diretto VLAN 10 -> VLAN 50
- Risultato
  - Il movimento laterale è bloccato; l'attacco è contenuto al PC infetto

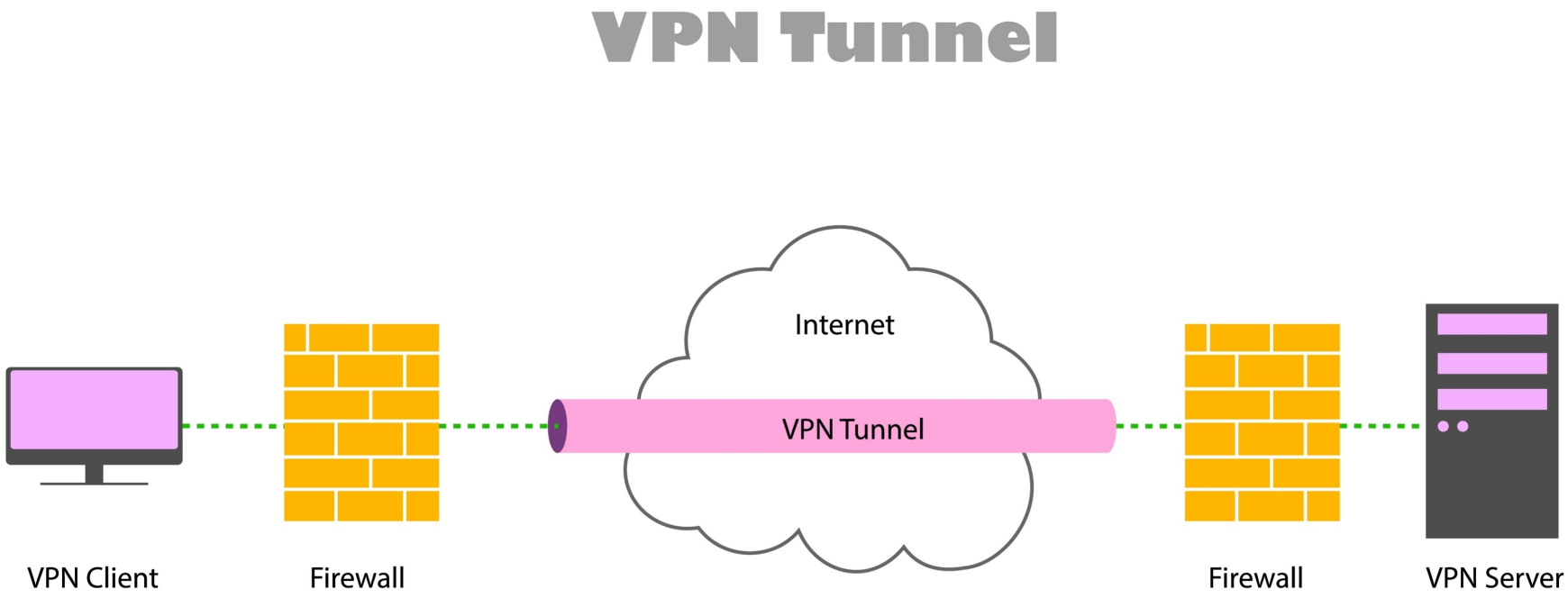
Segmentazione per Dispositivi IoT

- Problema
  - Dispositivi IoT (telecamere, smart TV) sono spesso insicuri e non patchabili
- Soluzione
  - Creare una VLAN dedicata e isolata ("IoT Zone")
- Policy
  - IoT -> Internet: Permesso (solo necessario)
  - IoT -> LAN Aziendale: Bloccato totalmente
  - LAN -> IoT: Permesso solo per gestione specifica
- Beneficio
  - Se una telecamera viene hackerata (botnet), non può attaccare i server aziendali

VPN (Virtual Private Network)

- Tunnel crittografato che estende una rete privata su una rete pubblica (Internet)
- Confidenzialità
  - I dati vengono cifrati (nessuno può leggerli in transito)
- Integrità
  - Garanzia che i dati non siano stati modificati durante il trasporto
- Autenticazione
  - Verifica dell'identità di chi accede al tunnel
- Utilizzi
  - Lavoro da remoto (Smart Working), connessione tra sedi distaccate

VPN (Virtual Private Network)



Tipologie di VPN

- Remote Access VPN (Client-to-Site)
  - Collega un singolo utente alla rete aziendale
  - Richiede software client sul dispositivo dell'utente
- Site-to-Site VPN
  - Collega intere reti (es Sede Milano con Sede Roma)
  - Trasparente per gli utenti finali; gestita dai gateway/router
- Protocolli Comuni
  - IPsec: Standard robusto, opera a livello 3
  - SSL/TLS (OpenVPN/Browser): Più flessibile per l'accesso client, opera a livello applicativo

VPN: Split Tunneling vs Full Tunneling

- Full Tunneling
  - Tutto il traffico dell'utente (anche navigazione personale) passa per la VPN aziendale
  - Pro
    - Massima sicurezza e monitoraggio
  - Contro
    - Alto consumo di banda aziendale
- Split Tunneling
  - Solo il traffico per le risorse interne passa per la VPN; il resto va diretto su Internet
  - Pro
    - Risparmio di banda
  - Contro
    - Il PC utente è esposto direttamente a Internet (rischio ponte)
- Best Practice
  - Full Tunneling per utenti ad alto rischio
  - Split Tunneling con endpoint protection robusto per gli altri

Autenticazione VPN Forte

- Il rischio
  - Una password VPN rubata garantisce accesso alla rete interna
- MFA (Multi-Factor Authentication)
  - Obbligatorio per qualsiasi accesso VPN
- Certificati Digitali
  - Utilizzo di certificati macchina per validare il dispositivo (non solo l'utente)
- Posture Check
  - La VPN verifica lo stato del PC prima di connettere (es Antivirus attivo? OS aggiornato?)
- Controlli contestuali
  - Blocco accessi da paesi anomali o orari sospetti (Geo-blocking)

Rischi e Mitigazione VPN

- Malware Tunneling
  - Un PC infetto connesso in VPN può infettare la LAN
- Soluzione
  - Segmentare gli utenti VPN in una VLAN specifica (non nella LAN generale)
- Furto credenziali
  - Phishing mirato agli accessi VPN
- Soluzione
  - Token hardware o app MFA
- Vulnerabilità Gateway
  - Mancato patching del concentratore VPN
- Soluzione
  - Aggiornamento firmware prioritario per i dispositivi di bordo
- Session Persistence
  - Sessioni che rimangono aperte troppo a lungo
- Soluzione
  - Time-out forzato e ri-autenticazione ogni 8-12 ore

Zone di Quarantena (Network Admission Control - NAC)

- Un'area di rete limitata dove vengono parcheggiati i dispositivi che non rispettano i requisiti di sicurezza.
  - Fase Pre-Admission: Il controllo avviene prima che il dispositivo riceva un IP valido o acceda alla rete.
- Criteri di Quarantena
  - Antivirus non aggiornato o disattivato.
  - Sistema operativo non patchato (es. Windows 7).
  - Rilevamento di traffico anomalo dal dispositivo.
  - Dispositivo sconosciuto (BYOD non registrato).

Funzionamento della Zona di Quarantena

- Isolamento
  - La VLAN di quarantena ha accesso solo ai Remediation Servers
- Accessi permessi in Quarantena
  - Server WSUS/Update per scaricare patch
  - Server Antivirus per aggiornare le firme
  - Portale Captive per scaricare l'agente di sicurezza
- Uscita dalla Quarantena
  - Automatizzata. Una volta soddisfatti i requisiti, lo switch sposta la porta sulla VLAN corretta

Aree di Contenimento (Incident Response)

- Differenza con Quarantena
  - La quarantena è preventiva/amministrativa; il contenimento è reattivo durante un attacco
- Obiettivo
  - Impedire che un incidente confermato si propaghi, senza spegnere necessariamente i sistemi (per preservare prove forensi)
- Strategie di Contenimento
  - Breve termine: Isolare i nodi infetti dalla rete (staccare cavo/port shutdown)
  - Lungo termine: Applicare patch, cambiare password, ricostruire sistemi puliti

Tecniche di Isolamento Avanzato

- VLAN di "Sinkhole"
  - Indirizzare il traffico malevolo verso un server che lo registra ma non risponde
- EDR Isolation
  - Utilizzare agenti Endpoint Detection & Response per isolare l'host via software
- L'host isolato comunica solo con la console di gestione EDR
- Sospensione VM: Se l'host è virtuale, mettere in pausa la macchina o fare uno snapshot della RAM prima di spegnere
- Blocco Account: Disabilitazione temporanea degli account utente/servizio compromessi in Active Directory

Esempio: Ransomware

- Rilevamento: L'IDS segnala traffico C&C (Command & Control) dal PC "Amministrazione-01"
  - https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/command-and-control-cac-attack/
- Automazione (SOAR - Security Orchestration, Automation, and Response): Il sistema di orchestrazione contatta lo switch
- Azione: La porta del PC "Amministrazione-01" viene spostata nella VLAN "Containment"
- Analisi: L'analista accede al PC in remoto (unica connessione permessa) per dump della memoria
- Bonifica: Reimaging del PC e ripristino dati da backup offline

Intrusion Detection System

- Sistema di monitoraggio che analizza il traffico alla ricerca di attività sospette
- Ruolo
  - È come una "telecamera di sorveglianza" o un allarme antifurto. Vede, registra, avvisa, ma NON ferma l'azione
- Posizionamento
  - "In parallelo" (TAP o SPAN port) rispetto al traffico. Non introduce latenza
- Modalità
  - NIDS (Network-based) analizza i pacchetti
  - HIDS (Host-based) analizza log e file di sistema
- Output: Genera alert per il SIEM (Security Information and Event Management) o gli analisti SOC (Security Operations Center)

Metodi di Rilevamento IDS

- Signature-Based (Firme)
  - Confronta il traffico con un database di attacchi noti (es. Snort rules)
  - Pro: Basso numero di falsi positivi per attacchi noti
  - Contro: Cieco contro gli attacchi Zero-day
- Anomaly-Based (Comportamentale)
  - Crea una "baseline" del traffico normale (es. volumi, orari, protocolli).
  - Segnala deviazioni (es. upload di 10GB alle 3 di notte).
  - Pro: Rileva minacce ignote
  - Contro: Alti falsi positivi.

Intrusion Prevention System

- Evoluzione dell'IDS che opera attivamente per bloccare le minacce rilevate
  - Ruolo: È come un "buttafuori". Ferma l'ingresso o l'azione malevola
  - Posizionamento: "In linea" (In-line) sul cavo di rete. Il traffico DEVE passare attraverso l'IPS
    - Se IPS lento, servizi applicativi lenti!!!
- Azioni IPS
  - Drop Packet (scarta il pacchetto)
  - Reset Connection (invia flag TCP RST per chiudere la sessione)
  - Block IP (aggiunge l'IP sorgente alla blacklist del firewall)

IDS vs IPS: Confronto Critico

- Impatto sulla rete
  - IDS: Nessun impatto (fail-open). Se si rompe, la rete funziona
  - IPS: Introduce latenza. Se si rompe o si blocca, la rete si ferma (fail-closed o fail-open a seconda della config)
- Rischio Falsi Positivi
  - IDS: Un falso positivo è solo un avviso fastidioso
  - IPS: Un falso positivo blocca traffico legittimo (Business Disruption)
- Utilizzo tipico
  - IDS per visibilità profonda
  - IPS per proteggere da exploit noti e gravi

Esempio Pratico: SQL Injection

- Attacco: Un hacker invia http://sito.com/login?user=' OR 1=1--
- Scenario con IDS
  - L'IDS vede la stringa malevola
  - Registra l'evento: "Alert: SQL Injection detected from IP X"
  - Il database riceve comunque la richiesta (possibile compromissione se non patchato)
- Scenario con IPS
  - L'IPS analizza il pacchetto in transito
  - Riconosce la firma dell'attacco
  - Scarta il pacchetto PRIMA che arrivi al Web Server
  - L'hacker riceve un timeout

Tuning e Gestione IDS/IPS

- La sfida del "Bias"
  - Troppi alert desensibilizzano gli analisti (Alert Fatigue)
- Tuning Iniziale: Avviare l'IPS in modalità "IDS-only" (solo monitoraggio) per 2-4 settimane
- Whitelisting: Escludere scanner di vulnerabilità autorizzati o traffico di backup dai controlli.
- Aggiornamento Firme: Deve essere quotidiano/automatico (Threat Intelligence feed).
- Correlazione: Integrare i log IDS/IPS con un SIEM per vedere il quadro completo.

Defense in Depth (Difesa in Profondità)

- Nessuna singola misura è sufficiente. Bisogna sovrapporre i controlli
  - Strato 1: Perimetro (Firewall, DDoS protection)
  - Strato 2: Rete (IDS/IPS, Segmentazione, DMZ, Proxy)
  - Strato 3: Endpoint (Antivirus, EDR, NAC/Quarantena)
  - Strato 4: Applicazione (WAF, Secure Coding)
  - Strato 5: Dati (Crittografia, Backup)

Riepilogo

- Firewall & Proxy: Filtrano e mascherano
- DMZ & Segmentazione: Isolano e riducono il danno
- VPN: Proteggono il transito remoto
- IDS/IPS: Rilevano e bloccano intrusioni
- Containment: Gestiscono l'incidente avvenuto

Conclusione: La Sicurezza come Conoscenza

- Oltre la difesa perimetrale
  - I firewall e le VPN sono inutili se non sappiamo cosa attraversa quei canali. La sicurezza non è un muro statico, è un processo cognitivo
- Visibilità Istante per Istante
  - L'obiettivo finale non è solo bloccare gli attacchi, ma avere una visione granulare e in tempo reale dello stato di salute del "sistema di servizi"
- I Tool come "Sensori"
  - L'IDS non serve solo a dare allarmi, ma a capire chi ci sta interrogando
  - La Segmentazione non serve solo a dividere, ma a evidenziare i flussi di traffico anomali tra reparti
- Dalla reazione alla comprensione
  - Solo conoscendo il comportamento "normale" dei servizi (baseline) possiamo identificare immediatamente una deviazione malevola o un guasto imminente

Non si può difendere ciò che non si vede. La vera sicurezza risiede nella conoscenza totale, istante per istante, di ciò che accade nella propria rete