TD SYNNEX

Next Generation FireWall

La protezione minima per la superficie di attacco

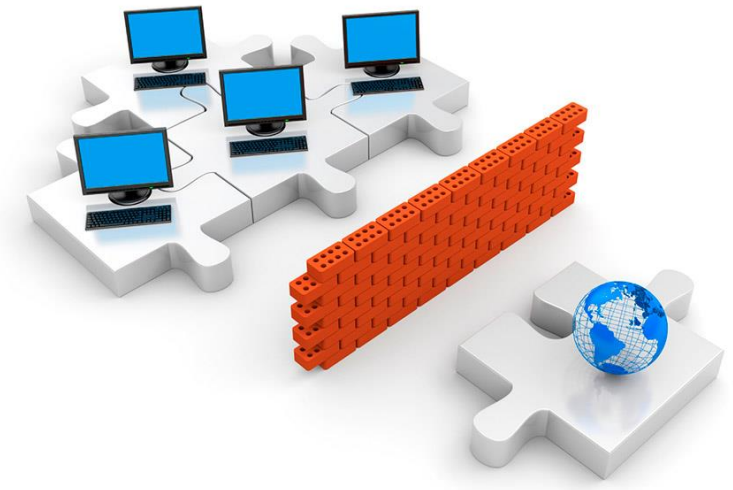
11 Ottobre 2024

Webinar

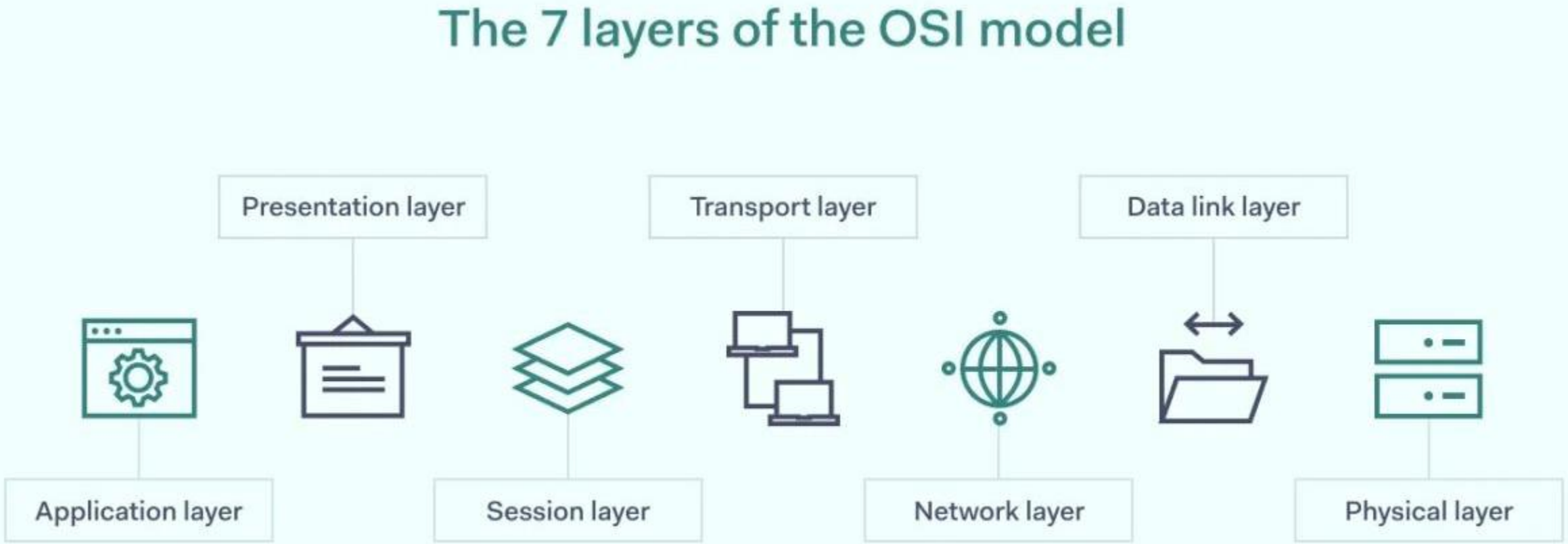
Andrea Pezzoni – Security Presales Specialist – TD SYNNEX

La protezione perimetrale

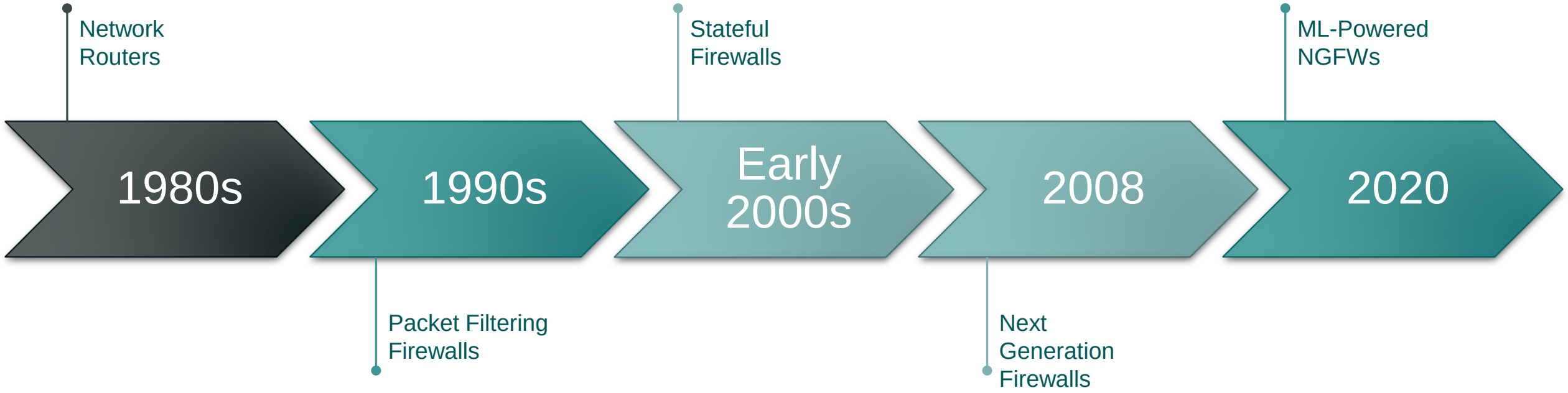
Il Firewall è un gateway inter-rete che limita il traffico di comunicazione dei dati da e verso una delle reti Collegate (quella detta “interna” al firewall) e quindi protegge le risorse di sistema di quella rete dalle minacce provenienti dall'altra rete (quella detta “esterna” al firewall).



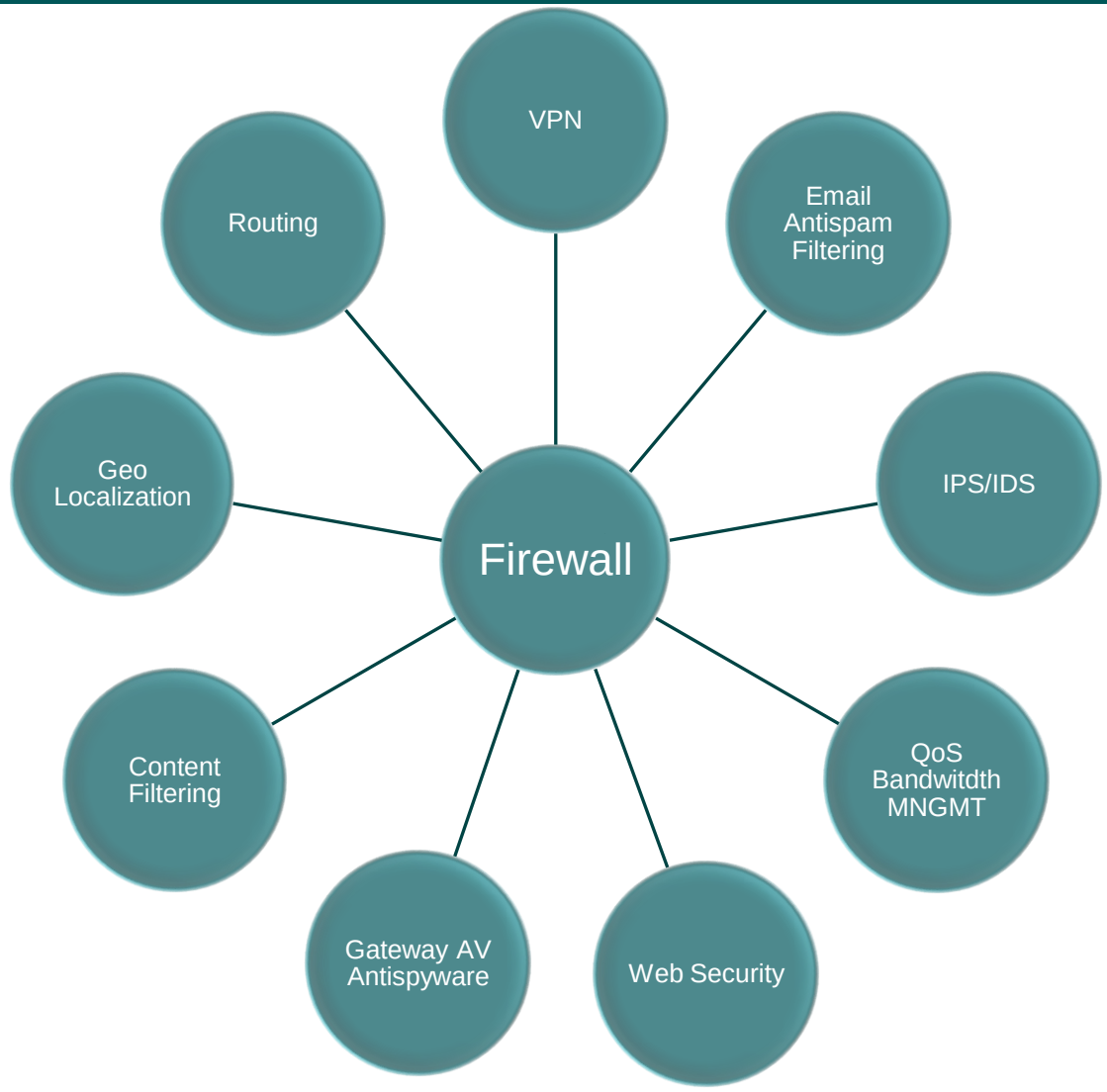
OSI Layer


The 7 layers of the OSI model
Presentation layer
Transport layer
Data link layer
Application layer
Session layer
Network layer
Physical layer

NGFW e i suoi «antenati»

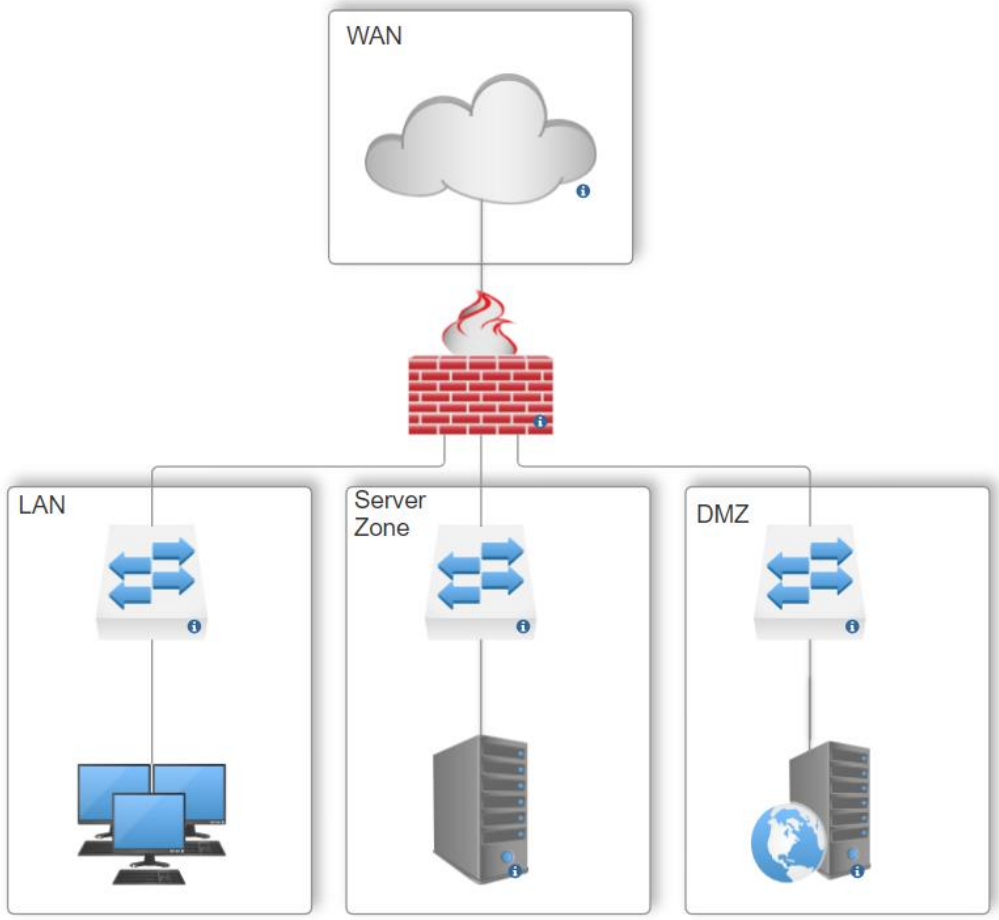


Firewall e Unified Threat Management

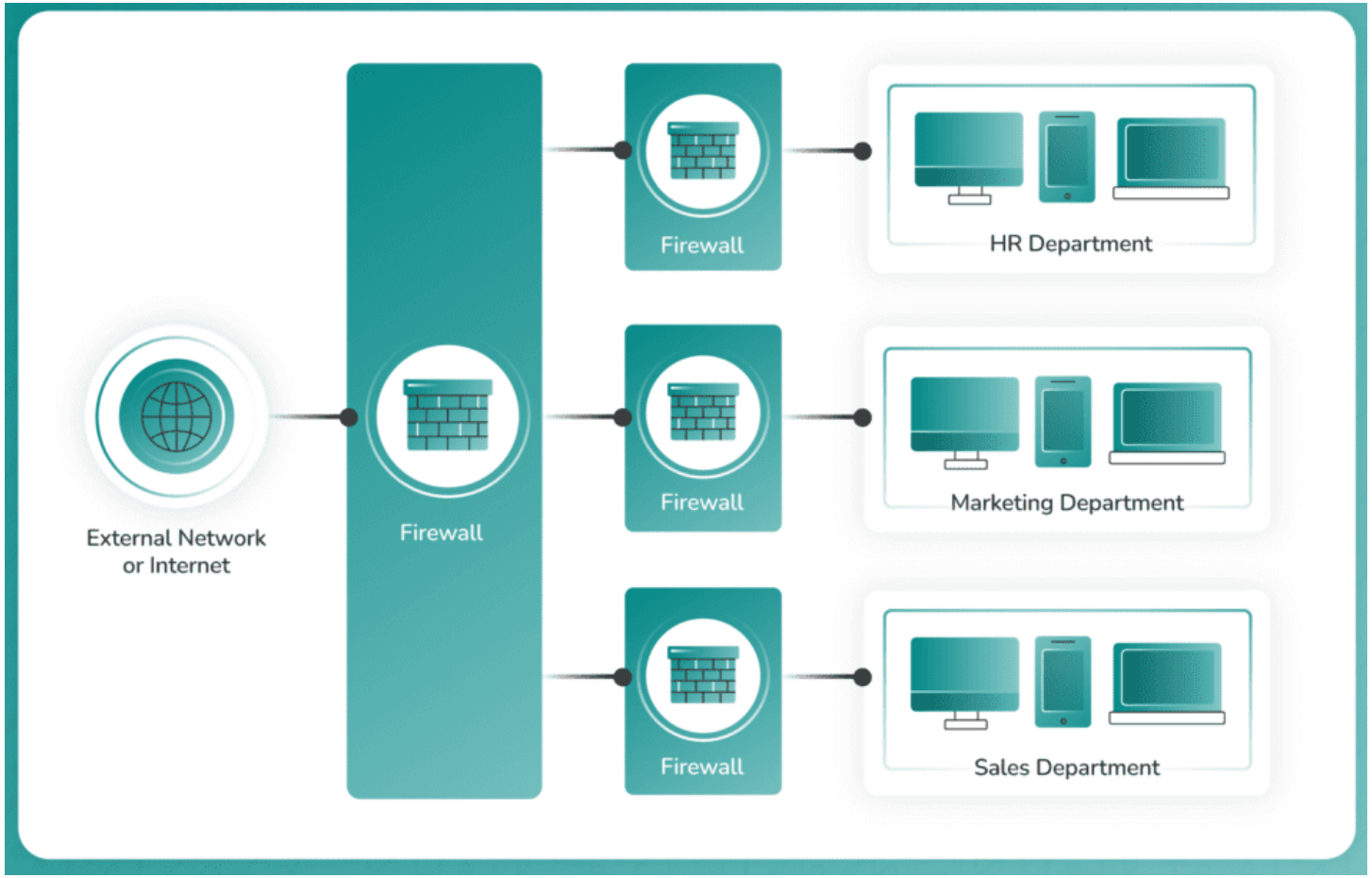


Protezione a Zone

Una zona è un gruppo di interfacce che hanno funzioni o caratteristiche simili.
Le zone stabiliscono i confini di sicurezza di una rete. Una zona definisce un confine in cui il traffico è soggetto a restrizioni di policy quando passa a un'altra regione della rete.
Un criterio di ispezione viene applicato al traffico che si sposta tra le zone.
I criteri interzona offrono una notevole flessibilità, per cui è possibile applicare criteri di ispezione diversi a più gruppi di host collegati alla stessa interfaccia del router.



Micro-Segmentazione

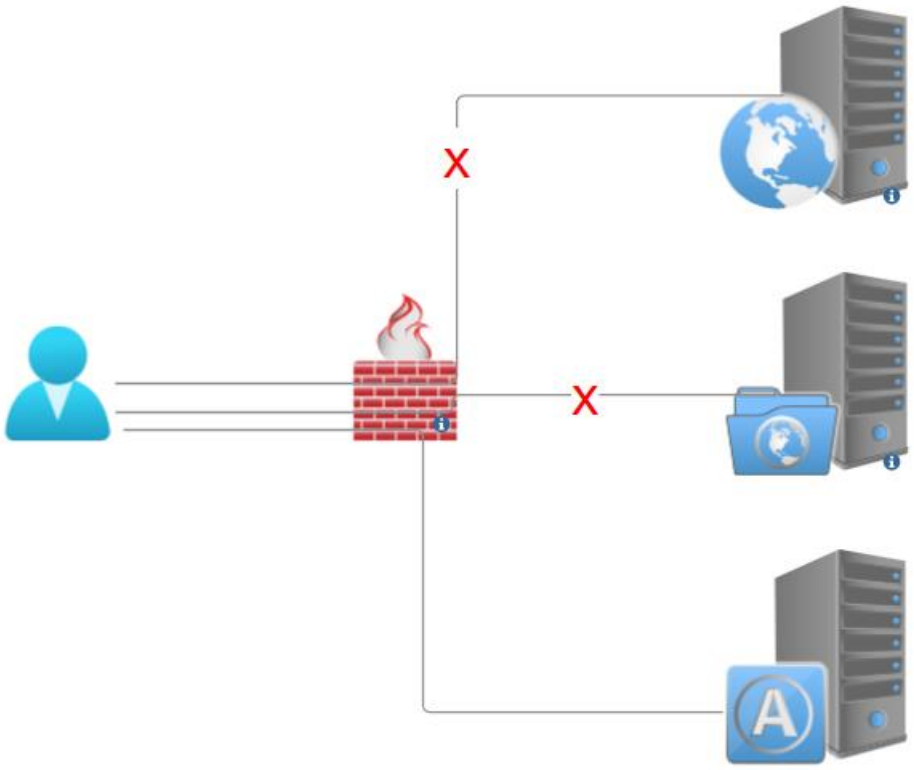


Zero Trust Network Access completa le policy di sicurezza introducendo il layer di Network e due concetti fondamentali:

Segmentazione e Microsegmentazione

- Mappare i dati e il traffico
- Determinare le esigenze di sicurezza
- Organizzare i segmenti per livello di rischio
- Dividere la rete in segmenti
  - Fisici
  - Logici
  - Servizi

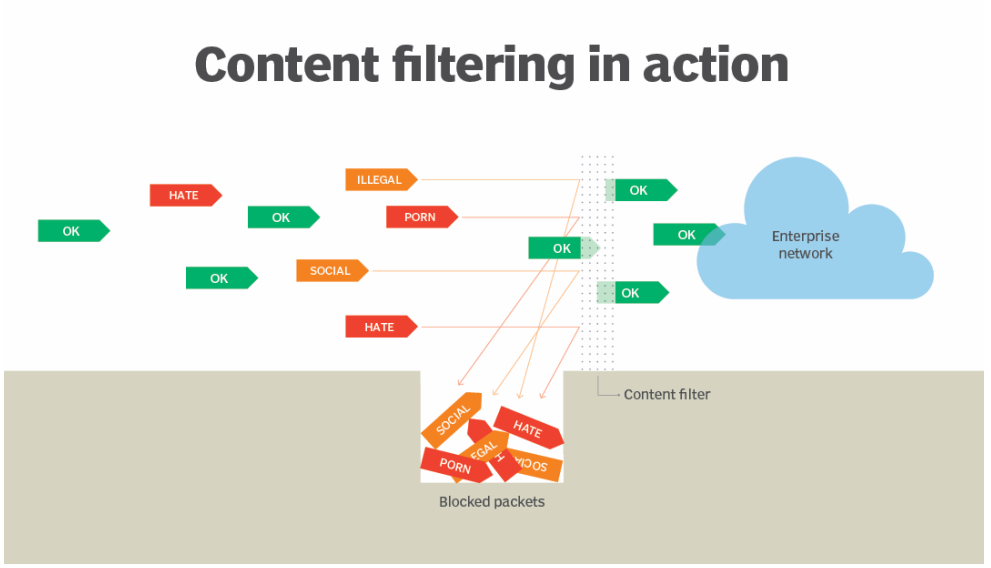
Accesso minimo



Il principio del minimo privilegio (PoLP) si riferisce a un concetto di sicurezza delle informazioni in cui a un utente vengono concessi i livelli minimi di accesso - o permessi - necessari per svolgere le proprie funzioni lavorative. È ampiamente considerato una best practice di cybersecurity ed è un passo fondamentale per proteggere l'accesso privilegiato a dati e risorse di alto valore.

Traffico IN e Traffico OUT

Deep Packet Inspection vs Content Filtering



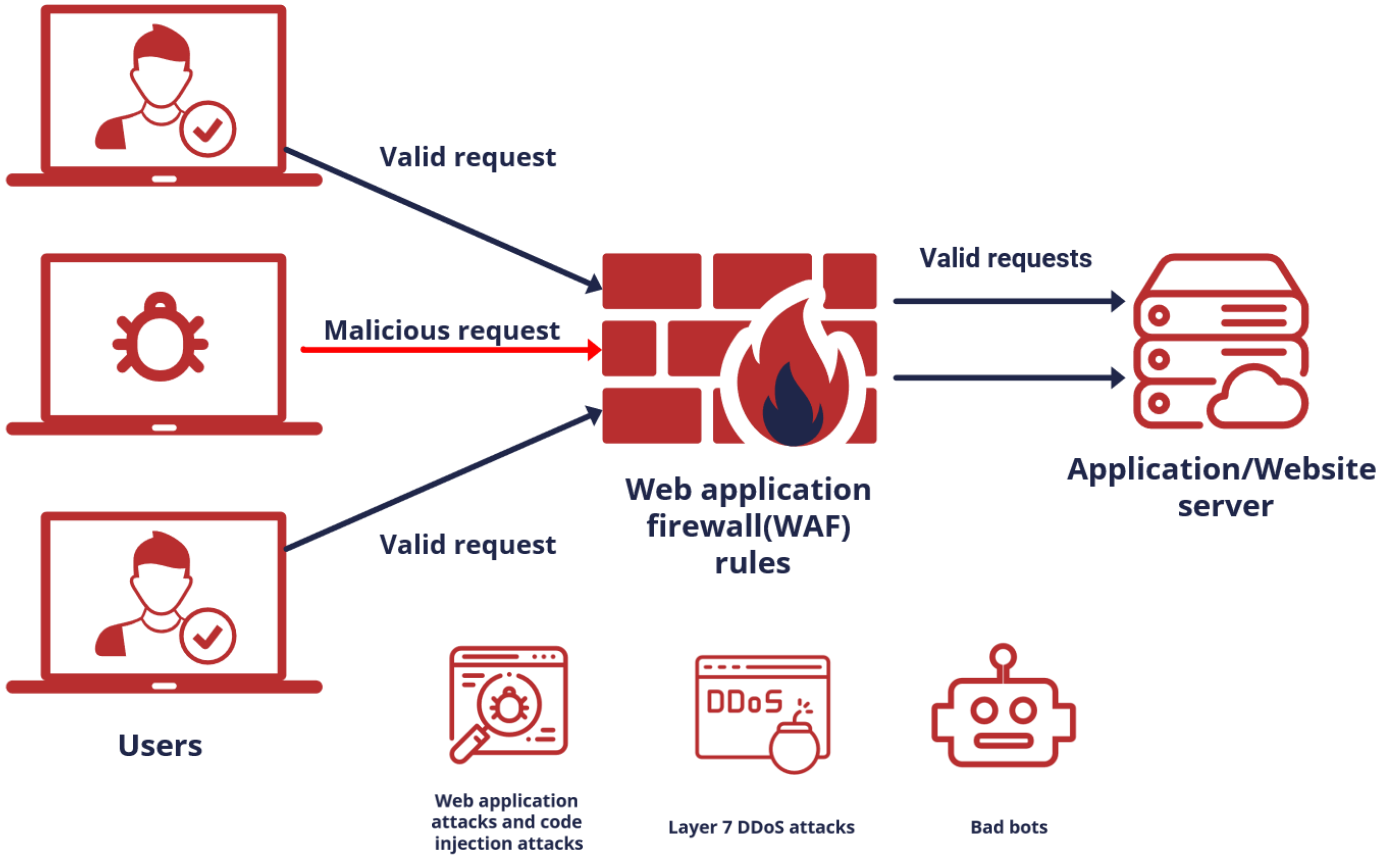
Firewall e Public Cloud

Obiettivi:
- Protezione da accessi non autorizzati
- Segmentazione e Access Control
- Filtro Applicazioni e Contenuti
- Prevenzione e Threat Detection
- Logging, Auditing e Compliance

Vantaggi:
- Aumento della sicurezza globale
- Scalabilità
- Controllo centralizzato delle policy
- Flessibilità e Agilità

Svantaggi:
- Complessità del disegno di network
- Potenziali falsi positivi
- Performance
- Single point of failure

WAF



- Protezione L7
- Scalabilità fondamentale contro DDOS
- Analisi del traffico vs code injection

TD SYNNEX

“As we’ve come to realize, the idea that security starts and ends with the purchase of a prepackaged firewall is simply misguided.”

Art Wittmann

https://csrc.nist.gov/glossary/term/firewall
https://www.paloaltonetworks.com/cyberpedia/history-of-firewalls
https://nordlayer.com/learn/firewall/layer-7/
https://sites.google.com/site/amitsciscozone/security/zone-based-policy-firewall
https://www.wallarm.com/what/unified-threat-management
https://www.cyberark.com/what-is/least-privilege/
https://www.techtarget.com/searchsecurity/definition/content-filtering
https://www.techtarget.com/searchnetworking/definition/deep-packet-inspection-DPI
https://www.itconvergence.com/blog/...of-firewalling-in-cloud-managed-services/
https://www.stormit.cloud/blog/what-is-a-web-application-firewall/

TD SYNNEX

Q&A

Your Opinion Counts!

Scarica la presentazione cliccando sul codice QR

PROSSIMI APPUNTAMENTI

18 OTTOBRE: IPS e IDS

25 OTTOBRE: TBD

https://forms.office.com/r/B8pN50j9f3

TEAM SECURITY: security.it@tdsynnex.com
SPEAKER: andrea.pezzoni@tdsynnex.com