Web/App/DB Katmanlı Ağ Segmentasyonu Planlama Şablonu — Yazılım / Sunucu ve Güvenlik (v1.0)

Asset Amaç: Bu şablon; DMZ, Web/Uygulama (App), Veritabanı (DB) ve Yönetim/Yedekleme/İzleme ağlarını mantıksal segmentlere (VLAN/Subnet) ayırıp Güvenlik Grubu (SG) ve Firewall kurallarını sürdürülebilir şekilde tasarlamak için hazırlanmıştır. Geçici olarak açılan güvenlik duvarı portlarının sistemde unutularak kalıcılaşması riskini "Kural Sahibi (Owner) + Otomatik Kapanış Tarihi" zorunluluğuyla ortadan kaldırır. Aynı zamanda KVKK/GDPR teknik tedbirleri uyarınca katmanlar arası erişim loglarının merkezi olarak doğru ve bütünlüklü saklanmasını sağlar.

Kim Kullanır?: Ağ Yöneticileri, Sistem Yöneticileri, DevOps / BT Liderleri ve Otel / B2B Altyapı Ekipleri.

Nasıl Kullanılır?

1. Altyapınızdaki segmentleri ve her segmentte yer alan varlık envanterini tanımlayarak internet erişim seviyelerini belirleyin.
2. Segmentler arası trafikte Default-Deny (varsayılan engelleme) prensibini esas alarak yalnızca gerekli Port/Protokol geçiş izin matrisini oluşturun.
3. Her güvenlik kuralına bir sorumlusu (owner), iş gerekçesi ve bitiş tarihi atayın; loglama ve KVKK uyum ayarlarını tamamlayın.

TEMPLATE — Katmanlı Ağ Segmentasyonu Planlama Şablonu

1) Segment Envanteri

Segment	Amaç	İçerik (Varlıklar)	İnternet Erişim Yönü	Owner
DMZ (Public)	Dış dünyaya açık servisleri barındırma	Nginx Reverse Proxy, Load Balancer, WAF	Gelen/Giden (Inbound/Outbound)	Network / Security
App (Private)	İş mantığı ve uygulama servislerini çalıştırma	Node.js, Java, Python API Container/VM	Yalnızca Giden (Outbound via NAT)	DevOps / App Team

DB (Isolated)	Hassas veri ve veritabanı yönetimi	PostgreSQL, MySQL, Redis Cluster	**İnternet Tamamen Kapalı**	DBA / Data Team
Mgmt (Management)	Sunucu ve ağ yönetim erişimi	Bastion Host, SSH Jump Server, VPN Gateway	Kısıtlı Giden / IP Whitelisted	SysAdmin Team
Monitoring	Sistem sağlık ve log toplama	Prometheus, Grafana, OpenSearch Agent	Kısıtlı Giden	SRE / Infrastructure
Backup	Sistem ve veritabanı yedekleme	Veeam, S3 Backup Gateway, NAS	Kısıtlı Giden (Encrypted)	SysAdmin / Storage

2) Segmentler Arası İzin Matrisi (Traffic Control)

Kaynak (Source)	Hedef (Destination)	Port / Protokol	İş Gerekçesi	Süre (Geçici mi?)
DMZ	**App**	TCP / 443 (HTTPS), TCP / 8080	Proxy trafiğini uygulama katmanına yönlendirme	**Kalıcı**
App	**DB**	TCP / 5432 (PostgreSQL), TCP / 6379	Uygulamanın veritabanı ve önbelleğe erişimi	**Kalıcı**

Mgmt	**DMZ / App / DB**	TCP / 22 (SSH), TCP / 3389 (RDP)	Güvenli Bastion Host üzerinden yönetim erişimi	**Kalıcı** (IP Kısıtlı)
Monitoring	**Tüm Segmentler**	TCP / 9100 (Node Exporter), TCP / 9090	Metrik ve sağlık durumu verilerini toplama	**Kalıcı**
App	**Backup**	TCP / 445 (SMB), TCP / 2049 (NFS)	Uygulama log ve medya yedeklerinin aktarımı	**Kalıcı**
External (Vendor)	**App (Staging)**	TCP / 8443	Dış entegrasyon sağlayıcısı test erişimi	**Geçici** (14 Gün)

3) Güvenlik Duvarı & Kural Yönetim Esasları

- **Default-Deny Politikası: Aktif (Evet)** — Tüm VLAN ve Güvenlik Gruplarında (SG) varsayılan olarak Deny All Traffic kuralı geçerlidir; sadece açıkça tanımlanan portlara izin verilir.
- **Geçici Kural Kapanış Tarihi Zorunlu: Evet** — Test veya üçüncü taraf erişimleri için açılan kurallara en fazla 30 günlük otomatik kapanma süresi (*TTL*) tanımlanır.
- **Kural Review Periyodu: 3 Ay (Çeyreklik)** — 90 günde bir aktif tüm güvenlik duvarı kuralları ve kural sahipleri (owners) denetlenir.
- **Değişiklik Onay Süreci:** Tüm kural değişiklikleri GitOps / Change Management biletine (Jira / Redmine) bağlanır; Güvenlik Lideri onayı olmadan prod firewall'una işlenemez.

4) Logging & KVKK Uyum Yönetimi

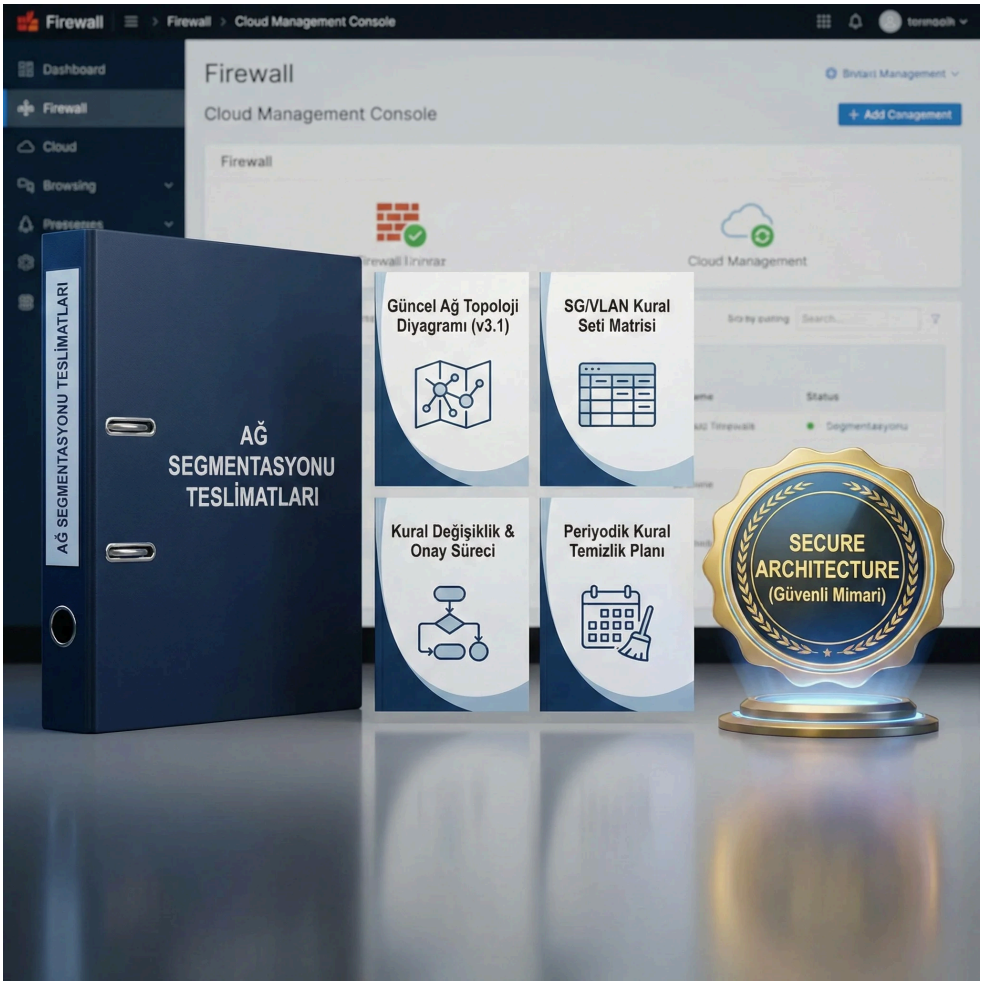
- **Segmentler Arası Erişim Logları Saklama Yeri:** Tüm Firewall / SG akış logları (VPC Flow Logs), WAF erişim kayıtları ve Bastion SSH oturum logları merkezi **OpenSearch / SIEM** sistemine aktarılır.
- **Log Saklama Süresi / Erişim Yetkisi:** Loglar minimum **2 Yıl (5651 ve KVKK gereği)** saklanır; erişim yetkisi yalnızca Güvenlik ve Denetim Ekipleri ile kısıtlıdır.
- **KVKK Uyum Notu:** DB segmentine erişimlerde kişisel verilerin (Örn: Müşteri/Misafir kayıtları) anonimleştirilmiş/maskelenmiş loglanması esastır. DB segmenti hiçbir koşulda doğrudan DMZ veya dış internete açılamaz.

5) Denetim ve Kontrol Listesi (Checklist)

- [ ] **Web DMZ'de, DB İç Segmentte:** DMZ sunucuları ile Veritabanı sunucuları farklı VLAN/Subnet'lerde izole edildi.
- [ ] **Web → DB Direkt Bağlantısı Kapalı:** DMZ katmanından DB katmanına doğrudan TCP/UDP erişimi güvenlik duvarı seviyesinde kesin olarak engellendi.
- [ ] **Mgmt / Backup / Monitoring Ayrı Ağda:** Yönetim, yedekleme ve izleme trafiği için ayrı IP blokları (VLAN/Subnet) tanımlandı.
- [ ] **Kurallarda Owner + Gerekçe + Kapanış Tarihi Mevcut:** Açılan her kural için bir sistem sorumlusu, Bilet No (Ticket) ve bitiş tarihi dökümante edildi.
- [ ] **Periyodik Kural Temizlik Planı Var:** Süresi dolan, artık kullanılmayan ve yetkisiz açılan portların tespiti için 3 aylık otomatik/manuel tarama süreci aktif.

Deliverables (Teslim Edilecek Çıktılar)

- **Katmanlı Ağ Mimari Şeması & VLAN Matrisi (v1.0):** Network topology, subnet blokları ve izolasyon sınırlarını gösteren mimari doküman.
- **Güvenlik Duvarı (Firewall / SG) İzin Kuralları Seti:** Nginx, AWS Security Group, Cloudflare ve Fortigate için uygulanabilir kural listeleri.
- **Kural Sorumluluk & Değişiklik Yönetimi (Change Control) Prosedürü:** Port açma/kapama taleplerinin onay, denetim ve kapatılma akış kılavuzu.
- **KVKK Uyumlu Merkezi Erişim & Flow Logging Konfigürasyonu:** Katmanlar arası trafiğin SIEM/OpenSearch üzerine aktarım ve saklama rehberi.



[Deliverables / Proof Card]

Ağ mimarları, siber güvenlik uzmanları ve DevOps liderleri için tasarlanmış, 1200x1200px (1:1) kare formatında yüksek çözünürlüklü bir Ağ Segmentasyonu Deliverables Kartı. Koyu karbon gri ve modern cam göbeği/mavi tonlarındaki teknolojik zemin üzerinde; DMZ, App ve DB katmanlarını gösteren 3 boyutlu izole ağ mimarisi şeması, güvenlik duvarı geçit simgeleri ve katmanlar arası kural matrisi diyagramı yer alıyor. Kartın üzerinde; "Web DMZ / App / Isolated DB Architecture", "Strict Default-Deny & SG Access Matrix", "Rule Ownership & Auto-Expiry Policy" ve "KVKK Compliant VPC Flow Logging & SIEM" teslimat kalemi başlıkları, yanlarında parlak mavi onay işaretleriyle scannable ve kurumsal bir proof-card formatında sergileniyor.