VPN + Bastion/SSM + SSO Erişim Mimarisi Planlama Şablonu — Yazılım / Sunucu ve Güvenlik (v1.0)

Asset Amaç: Bu şablon; sunucu altyapılarına doğrudan SSH/RDP erişimini tamamen kapatıp, tüm erişim kanallarını VPN + Bastion Host / AWS SSM + SSO (Single Sign-On) ve RBAC (Rol Bazlı Erişim Kontrolü) kombinasyonuyla merkezileştirmek ve kayıt altına almak için hazırlanmıştır. Dış ajans, yüklenici ve partner erişimlerini süreli, sınırlı ve anında geri alınabilir bir yapıya kavuşturarak offboarding süreçlerini standartlaştırır. Gerçekleştirilen tüm komut ve oturum kayıtlarını KVKK teknik tedbirleri ve 5651 sayılı kanun şartlarıyla uyumlu adli izleme katmanına bağlar.

Kim Kullanır?: BT/DevOps Ekipleri, Siber Güvenlik / Ops Birimleri, Otel IT Yöneticileri ve B2B Platform Yöneticileri.

Nasıl Kullanılır?

1. Organizasyonel rollere, ortamlara ve sunucu gruplarına göre erişim matrisini (RBAC) doldurun.
2. SSO kimlik doğrulama, VPN ve Bastion/SSM geçiş mimarisini kurgulayıp oturum kayıt (*logging*) ve SIEM noktalarını işaretleyin.
3. Süreli yetkilendirme, onay akışları, offboarding (işten ayrılış/proje bitimi) adımlarını ve acil durum (*break-glass*) prosedürünü runbook'a kitleyin.

TEMPLATE — VPN + Bastion/SSM + SSO Erişim Mimarisi Planlama Şablonu

1) Organizasyon ve Kapsam Tanımlama Formu

Parameter	Detay / Giriş Alanı
Proje Tipi	[ ] Otel Operasyon (PMS/Web/WiFi) | [ ] B2B SaaS Platform | [ ] Ajans Altyapısı
Hedef Ortamlar	[ ] Development | [ ] Staging | [ ] Production
Sunucu Grupları	[ ] Web (Nginx/Frontend) | [ ] App (API/PMS) | [ ] DB (Postgres/Redis) | [ ] Diğer

Remote Ekip / Partner Var mı?	[ ] Evet (Süreli/Sözleşmeli) | [ ] Hayır (Yalnızca İç Ekip)

2) Rol Matrisi (RBAC — Rol Bazlı Erişim Kontrolü)

Kullanıcı rollerine göre erişim hedefleri, yetki seviyeleri ve onay mekanizması tablosu:

Rol	Ortam	Erişim Hedefi	Yetki Seviyesi	Süre	Onay Sorumlusu
DevOps Mühendisi	Prod / Staging	Tüm Sunucu Grupları	Sudo / Admin (Full)	Sürekli	IT Director / Lead
Backend Geliştirici	Staging / Dev	Web & App Servers	User (No-Sudo)	Sürekli	Team Lead
Veri Analisti / BI	Production	DB Server (Read-Only)	ReadOnly SQL	8 Saat (Masa başı)	Data Owner
Dış Ajans / Yüklenici	Staging	Belirli Web/App Dizinleri	Restricted / Chroot	Proje Süresince (30 Gün)	BT Güvenlik Sorumlusu
Stajyer / Jr. Dev	Development	Dev App Server	Read / Exec (Kısıtlı)	Mesai Saatleri (9:00-18:00)	Kıdemli Geliştirici
Acil Durum (Break-Glass)	Production	All Infra (Console)	Root / Emergency	Max 2 Saat	CISO / CTO

3) Erişim Akışı (VPN + Bastion/SSM + SSO Mimari Kurgusu)

- **SSO (Single Sign-On) Sağlayıcı:** Google Workspace / Microsoft Entra ID (Azure AD) / Okta *(MFA/TOTP Zorunlu)*.
- **VPN Modeli:** WireGuard / OpenVPN / Tailscale ZTNA *(Sadece Bastion/SSM IP'lerine tünelleme)*.
- **Bastion / SSM Seçimi:**
  - Cloud: AWS Systems Manager (SSM) Session Manager *(Port 22 açmadan agent üzerinden yetkilendirme)*.
  - On-Prem / Hybrid: OpenSSH Teleport veya Hardened Linux Bastion Host *(SSH Jump Box)*.
- **Doğrudan SSH / RDP Kapatma Planı:** Production ve Staging sunucularında 0.0.0.0/0 IP aralığına SSH (Port 22) ve RDP (Port 3389) erişimi güvenlik duvarından tamamen engellenir. Yalnızca Bastion IP'si veya SSM Agent iletişimine izin verilir.

4) Oturum Logging & Adli Audit (KVKK ve 5651 Uyumlu)

- **Oturum Kaydı Nerede Tutulacak?:** AWS S3 (WORM / Object Lock ile değiştirilemez kova) veya Şifreli Merkezi Syslog Sunucusu.
- **SIEM Entegrasyonu var mı?:** [X] Evet *(Wazuh / Elastic SIEM / Splunk ile anlık log analizi)*.
- **Log Saklama Süresi ve Erişim Yetkisi:**
  - Saklama Süresi: KVKK ve 5651 teknik tedbir standartlarına uygun olarak **565 gün (2 Yıl)** boyunca saklanır.
  - Erişim Yetkisi: Yalnızca BT Güvenlik Yöneticisi ve DPO (Veri Koruma Görevlisi) inceleme yetkisine sahiptir.

5) Offboarding ve Yetki Geri Alma Prosedürü

- **Süreli Erişim Mekanizması:** Dış ajans ve dönemsel personel için IAM politikalarında veya Teleport üzerinde otomatik sona eren (*TTL - Time to Live*) erişim biletleri atanır.
- **Çalışan Ayrılınca Kapatma Adımı:** İK portalı üzerinden işten çıkış kaydı girildiği an SSO (Entra ID/Google) hesabı askıya alınır; bağlı tüm VPN, Bastion ve AWS SSM yetkileri anında iptal olur.
- **Ajans İşi Bitince Kapatma Adımı:** Proje bitim tarihinde sözleşmeli erişim hesabı otomatik pasife çekilir, SSH yetkilendirme anahtarları (*Public Keys*) sunuculardan kaldırılır.
- **Break-Glass (Kriz Anı) Prosedürü:** Kimlik doğrulama veya VPN servisleri çöktüğünde kullanılmak üzere, fiziksel kasada mühürlü saklanan 2 parçalı (*Dual-Control*) acil durum anahtarları ile erişim sağlanır ve her saniyesi adli loga kaydedilir.

6) Denetim ve Kontrol Listesi (Checklist)

- [ ] **Prod'da Public SSH / RDP Kapalı:** İnternete açık tüm Port 22 ve 3389 girişleri kapatıldı.
- [ ] **SSO + MFA Zorunlu Kılındı:** Tüm yetkili girişlerinde Donanım Anahtarı (YubiKey) veya Authenticator zorunluluğu getirildi.
- [ ] **Bastion / SSM Tek Giriş Kanalı Yapıldı:** Sunuculara doğrudan erişim engellenerek tek geçit noktası (*single choke point*) sağlandı.
- [ ] **Oturum Kayıtları Merkezi Yapıldı:** Kullanıcıların attığı tüm komutlar ve ekran oturumları değiştirilemez merkezi sunucuya aktarılıyor.

- [ ] **Ajans Erişimi Süreli ve Rol Bazlı:** Dış tedarikçilere süresi kısıtlı ve izole edilmiş yetkiler tanımlandı.
- [ ] **Offboarding Tek Noktadan Bağlandı:** SSO hesabının kapatılmasıyla tüm altyapı erişimlerinin anında kesildiği doğrulandı.

Deliverables (Teslim Edilecek Çıktılar)

- **VPN + SSM + SSO Merkezi Erişim Planlama Şablonu (v1.0):** Rol matrisini ve bağlantı mimarisini tanımlayan teknik planlama belgesi.
- **RBAC & Erişim Onay Politikası Dokümanı:** Kullanıcı seviyelerine göre onay mercilerini ve erişim sürelerini gösteren kural kütüphanesi.
- **Adli Audit & Log Saklama Prosedürü:** Oturum kayıtlarının KVKK ve 5651 teknik tedbirlerine uygun güvenliğini sağlama rehberi.

[Deliverables / Proof Card]

DevOps mimarları, BT güvenlik uzmanları ve sistem yöneticileri için tasarlanmış, 1200x1200px (1:1) kare formatında yüksek çözünürlüklü bir Kimlik ve Erişim Yönetimi (IAM) teslimat kartı. Koyu karbon gri ve siber güvenlik mavisi tonlarındaki teknolojik zemin üzerinde, SSO kimlik doğrulama ikonu, kilitli VPN tüneli simgesi, AWS SSM agent logosu ve adli log kayıt kalkanı görselleri yer alıyor. Kartın üzerinde; "Merkezi SSO + MFA Doğrulama Katmanı", "Port 22/3389 Kapalı - SSM/Bastion Tunnel", "Tam Kapsamlı Oturum & Komut Logging" ve "Otomatik Offboarding & Süreli Ajans Erişimi" teslimat kalemi başlıkları, yanlarında parlak onay işaretleriyle scannable ve kurumsal bir proof-card formatında sergileniyor.