

Masoud Kimiaei

Senior Network Security Architect | Zero Trust & Enterprise Security Design

Tehran, Iran

Professional Summary

Senior Network Security Architect with over 10 years of progressive experience designing, governing, and evolving enterprise and carrier-grade security architectures across banking, telecom, ISP, and large-scale enterprise environments. Specialized in Zero Trust Architecture, network segmentation, NGFW design, WAF and application security, DDoS protection, and secure application delivery, with a strong architectural focus on blast radius reduction, Assume Breach principles, and security-by-design methodologies.

Demonstrates deep architectural expertise across Palo Alto Networks, Fortinet Security Fabric, and F5 BIG-IP platforms, designing resilient North-South and East-West traffic control models aligned with NIST Cybersecurity Framework, NIST SP 800-207 (Zero Trust), ISO/IEC 27001, OWASP Top 10, and PCI DSS architectural principles. Experienced in building zone-based security models, internal segmentation firewalls (ISFW), multi-tier DMZ architectures, and high-availability security designs that balance protection, performance, and operational sustainability.

Recognized for translating business, regulatory, and operational risk into enforceable and scalable security architectures, bridging executive-level strategy with hands-on technical execution. Applies a pragmatic, risk-driven mindset that prioritizes resilience over prevention, visibility over obscurity, and architectural clarity over tool-centric complexity, enabling organizations to operate securely at scale in mission-critical environments.

Security Architecture Standards & Frameworks

Zero Trust Architecture

- NIST SP 800-207 (Zero Trust Architecture)
- Assume Breach methodology
- Least Privilege & Explicit Trust
- Trust Zone & Trust Boundary definition
- Micro-segmentation and lateral movement control

NIST Frameworks

- NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover)
- NIST SP 800-41 – Firewalls and Firewall Policy
- NIST SP 800-53 – Security & Privacy Controls
- NIST SP 800-61 – Incident Response Lifecycle
- NIST SP 800-92 – Logging and Monitoring

Enterprise Network Security Architecture

- Defense-in-Depth
- North–South and East–West traffic segmentation
- DMZ and multi-tier application architectures
- No-Bypass and Symmetric Routing principles
- Blast Radius reduction
- High Availability (HA) & Disaster Recovery (DR)

Application & Web Security

- OWASP Top 10
- OWASP API Security Top 10
- WAF architecture (Positive / Negative security models)
- Layer-7 behavioral protection

Compliance & Governance

- ISO/IEC 27001 (ISMS concepts, risk treatment, control alignment)
 - ISO/IEC 27002
 - GDPR (Data Protection by Design & by Default)
 - PCI DSS (Architectural alignment, segmentation, scope reduction)
-

Vendor Architecture Expertise

Palo Alto Networks

- Zone-Based Firewall Architecture
- App-ID, User-ID, Content-ID
- Internal Segmentation Firewall (ISFW)
- Zero Trust Network Security enforcement

Fortinet Security Fabric

- FortiGate NGFW architecture
- Secure SD-WAN design
- FortiAnalyzer & FortiManager (centralized visibility)

F5 BIG-IP

- LTM, AWAFF, AFM, DNS, APM
 - Application delivery and security design patterns
 - SSL offloading and traffic optimization
-

Professional Experience

Network Security Manager

Manetco | Tehran, Iran

Apr 2025 – Present

- Designed enterprise-scale network security architectures using FortiGate and F5 BIG-IP
 - Defined trust boundaries, segmentation models, and secure traffic flows
 - Implemented WAF, VPN, and high-availability designs
 - Conducted architectural risk assessments and mitigation planning
-

Senior Network Security Consultant

Central Bank of Iran | Tehran, Iran

Oct 2024 – Present (Part-time)

- Architected F5 BIG-IP infrastructure (LTM, AWAFF, AFM, DNS)
 - Designed secure exposure of mission-critical banking applications
 - Aligned application security with OWASP and Zero Trust principles
-

Network & Security Manager

Hesabo | Tehran, Iran

May 2024 – Apr 2025

- Defined enterprise security architecture aligned with business objectives
- Led risk assessment and incident response architecture
- Supported ISO 27001 and GDPR compliance initiatives

Senior Network Security Consultant

Amn Pardazan Sorena | Tehran, Iran

Dec 2022 – Present (Part-time)

- Designed firewall and WAF architectures for enterprise customers
- Implemented F5 LTM for resilient application delivery
- Delivered Fortinet Security Fabric designs

Cyber Security Consultant

MTN Irancell | Tehran, Iran

Nov 2023 – Present

- Provided security architecture consulting for Fortinet and F5 platforms
- Supported infrastructure hardening and application security design

Network Security Manager

Sapra Sanat | Tehran, Iran

Aug 2020 – Nov 2023

- Designed enterprise NGFW and DDoS protection architectures
- Led security architecture decisions for critical infrastructure
- Guided technical teams on secure network design

Cyber Security Consultant

RighTel | Tehran, Iran

Jun 2020 – Aug 2022

- Designed telecom-grade security architectures
- Implemented NGFW and WAF solutions

Cyber Security Consultant

Shatel | Tehran, Iran

Feb 2019 – Jul 2020

- Designed ISP security architectures using FortiGate and F5 BIG-IP

Network Security Engineer

Sapra Sanat | Tehran, Iran

Jul 2014 – Aug 2020

- Implemented NGFW, VPN, and IPS solutions
- Built strong foundations in secure network design and operations

Training & Instruction Experience

Senior Technical Instructor | Network & Cyber Security

3000+ Hours of Professional Training Delivery

Delivered advanced, hands-on, scenario-based training for enterprise engineers, security teams, and consultants, emphasizing architecture-first thinking, real-world attack scenarios, and production-grade designs.

Training Domains

- **F5 BIG-IP:** LTM, AWAFF/ASM, AFM, DNS, APM, SSL Offloading, ADC Architecture
- **Fortinet:** FortiGate, FortiWeb, FortiAnalyzer, FortiManager, Secure SD-WAN
- **Palo Alto Networks:** NGFW Architecture, Zone-Based Design, App-ID, User-ID, ISFW, Zero Trust
- **Cisco:** CCNA, CCNP Security, Firepower (FTD)
- **Cybersecurity:** CEH v12, CompTIA Security+, CompTIA Network+, OWASP Top 10

Training Methodology

- Architecture-first and risk-driven approach
- Attack → Failure → Analysis → Mitigation learning model
- Real-world enterprise and banking scenarios
- Strong focus on **Why before How**

Education

B.Sc. in Computer Software Engineering

University of Science and Culture – Tehran, Iran

Architecture Design Philosophy

Security architecture is not about preventing all breaches; it is about limiting impact, controlling blast radius, and ensuring survivability. Architecture must precede technology, risk must precede rules, and every allowed flow must have a clear business justification