redesign

SERVICE BRIEF

Network Security Assessment & Architecture Review

re

This document outlines the scope, deliverables, responsibilities, and terms governing Redesign's Network Security Assessment & Architecture Review Services.

This engagement provides a structured evaluation of an organization's current network design, security controls, segmentation strategy, and supporting technologies to identify gaps, misconfigurations, or exposure risks and provide actionable recommendations for improvement.

This service engagement is governed by this Service Brief and associated with SKU: SEC-NET-ASSESS. The quantity defined in the quote reflects the number of sites to be assessed.

The FUTURE BELONGS
to the CURIOUS.

Table of Contents

01. Services Overview

Redesign's Network Security Assessment & Architecture Review provides a technical evaluation of network infrastructure, security controls, and traffic flows with the goal of identifying weaknesses, outdated configurations, overexposed assets, or opportunities for improved segmentation and control.

The assessment is performed through documentation review, stakeholder interviews, and inspection of network control systems such as firewalls, switches, VPNs, and segmentation strategies.

02. Offer Structure

PRIMARY SERVICES

- Architecture review of current state network design and segmentation
- Evaluation of perimeter and internal network security controls
- Assessment of VPN, remote access, and internet edge exposure
- Analysis of firewall rules, ACLs, and zoning strategies
- Recommendations for hardening, modernization, or re-segmentation

OPTIONAL ADD-ONS

Separate SOW

- Network diagram creation or updates
- Firewall rulebase cleanup or design
- Zero Trust network planning
- Integration with vulnerability assessment

03. Project Scope

The assessment is scoped to the number of environments or network zones defined in the quote. Redesign will analyze the topology, edge controls, segmentation approach, traffic flows, and device-level configurations (where provided).

Examples of Scoped Sites/Zones/Environments

- Corporate office networks
- Cloud VPCs or VNets (AWS, Azure, GCP)
- Data centers
- Remote access or VPN infrastructure
- Industrial or OT environments
- VPN and wireless network connectivity
- User account provisioning and permissions management
- Operating system and patch health for endpoints

04. Quantity & Effort Model

- **Service SKU: SEC-NET-ASSESS**
- **Quantity: Number of sites/zones/environments to be assessed**
- **Work per Unit Includes:**
  - One full analysis of a defined site, zone or network boundary

INCLUDED

Quantity of 3 may include the Customer's HQ network, Azure virtual network, and VPN remote access environment.

05. Services & Key Activities

Stage	Key Activities
Discovery & Planning	▪ Review scope and define environment boundaries ▪ Request network diagrams, device configurations, and access ▪ Schedule stakeholder interviews (network and security leads
Architecture & Control Review	▪ Evaluate segmentation, zoning, and interconnectivity ▪ Assess firewall rulesets and access control models ▪ Review ingress/egress points, NAT, and exposure ▪ Identify use of encryption, IDS/IPS, and traffic inspection
Risk & Gap Analysis	▪ Identify architectural risks or inefficiencies ▪ Detect overly permissive rules, exposed services, or shadow access ▪ Review against best practices and relevant frameworks (e.g., Zero Trust, NIST)
Recommendations & Reporting	▪ Provide prioritized risk-based remediation actions ▪ Suggest architectural improvements or control updates ▪ Deliver annotated diagrams (if in scope) and reporting

06. Deliverables

Executive Summary with key risks and opportunities

Technical Findings Report per environment

Remediation Recommendations Roadmap

Stakeholder Review Session (virtual, 1 hour)

07. Services Scope Changes

Expanding to additional environments, re-assessing new architectures, or adding firewall rulebase analysis may require a revised quote or separate SOW.

---

08. Services Scope Exclusions

This engagement does not include:

- **Real-time monitoring or intrusion detection**
- **Configuration of firewalls or other network devices**
- **Vulnerability scanning or penetration testing (available separately)**
- **Documentation of undocumented networks unless included in scope**

---

09. Customer Responsibilities

- **Provide accurate and current network diagrams (or allow Redesign to build from interviews)**
- **Provide access to relevant device configurations or read-only dashboards**
- **Assign technical stakeholders for interviews**
- **Review and approve project scope and deliverables**

Failure to meet these requirements will prevent Redesign from delivering the services outlined in this Service Brief.

10. Services Schedule

- **Start Date:**
  Upon signed quote and completion of discovery inputs
- **Delivery:**
  Final report submitted and reviewed in scheduled session

---

11. Terms and Conditions

This engagement will be governed by the Seller's terms and conditions located at:

SERVICES WILL NOT BEGIN UNTIL THE FOLLOWING PREREQUISITES ARE MET

- Signed quote referencing SKU: SEC-NET-ASSESS and quantity
- Access to diagrams, configs, and key stakeholders
- Confirmation of scoped network zones

Failure to meet these requirements will prevent Redesign from delivering the services outlined in this Service Brief.

redesign

The FUTURE BELONGS
to the CURIOUS.