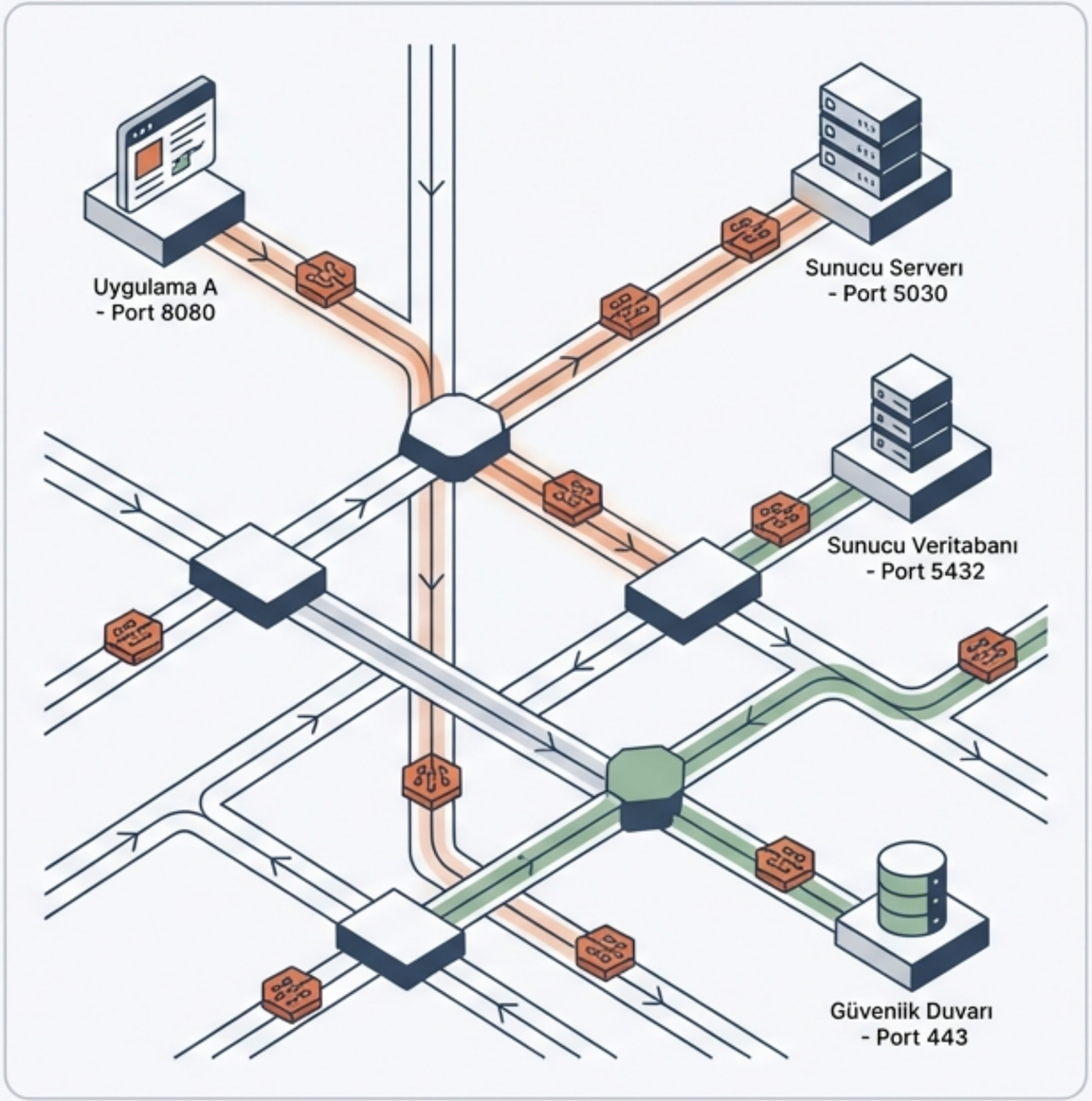
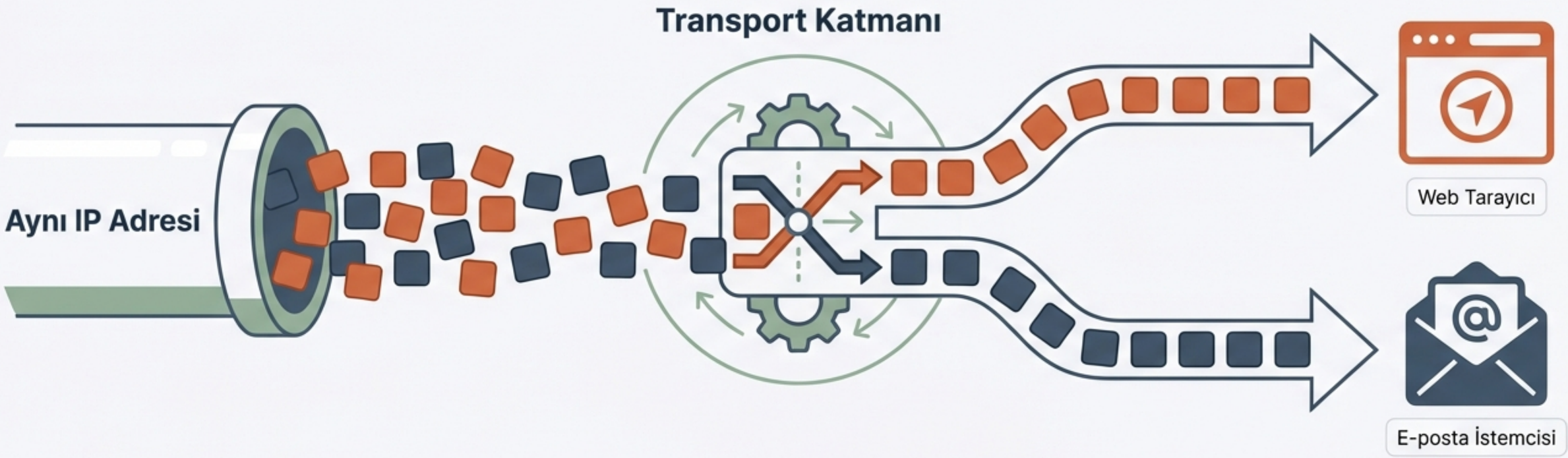
Ağ İletişiminin Temelleri: Port ve Soket Kavramları

Veri paketlerinin doğru uygulamalara nasıl ulaştığının ve siber güvenlikteki kritik rollerinin incelenmesi.



Neden Portlara İhtiyacımız Var?

Tek bir cihazda aynı anda hem web'de geziniyor hem de e-posta alıyorsunuz. Tüm veri paketleri aynı IP adresine gelir. Transport (Taşıma) katmanı bu paketleri uygulamalara nasıl doğru şekilde dağıtır?



Cevap: Port Numaraları

Port Kavramı: Bina ve Kapı Analojisi

IP Adresi = Bina Adresi

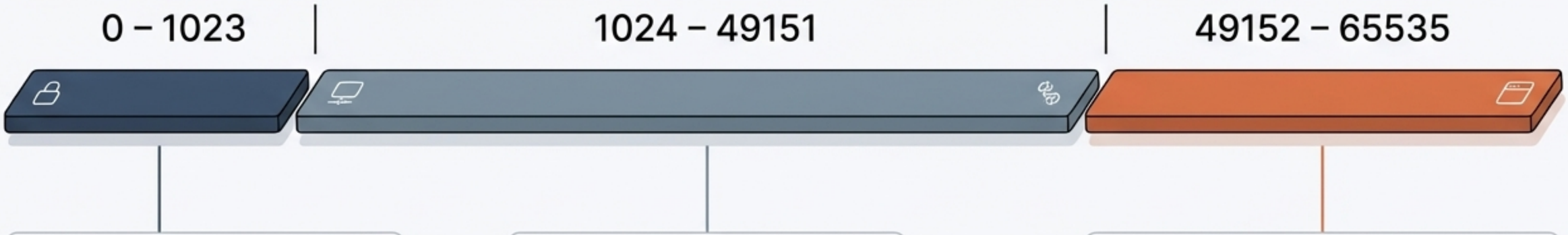
Ağ üzerindeki cihazı (sunucu veya bilgisayar) bulmayı sağlar.

Port Numarası = Oda Kapısı

O cihazda çalışan spesifik servisi veya uygulamayı bulmayı sağlar.

Örnek: 192.168.1.10:80 → Cihaza git (IP), Web sunucusunun kapısını çal (Port 80).

Port Aralıkları ve Kategorileri (0 – 65535)



Well-known Ports (İyi Bilinen Portlar)

IANA tarafından atanır. Genellikle standart sunucu servisleri (Web, E-posta) içindir.

Registered Ports (Kayıtlı Portlar)

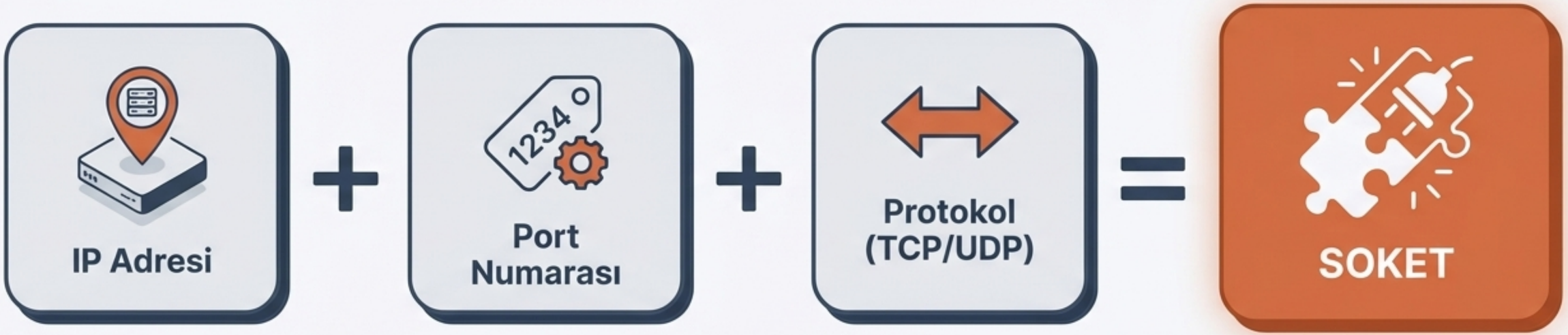
Belirli uygulamalar ve yazılımlar tarafından kullanılmak üzere rezerve edilmiştir.

Dynamic / Ephemeral Ports (Dinamik/Geçici Portlar)

İstemci (client) uygulamaları tarafından geçici bağlantılar için işletim sistemi tarafından otomatik olarak atanır.

Soket (Socket) Nedir?

Soket, iki bilgisayar arasındaki sanal TCP veya UDP iletişim kanalının yazılımsal karşılığıdır.

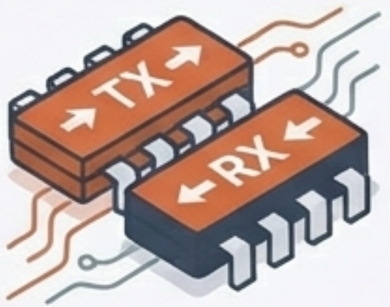


- Ağ üzerinden mesajların geçtiği fiziksel olmayan kapı eşiğidir.
- Her bağlantı için işletim sistemi tarafından oluşturulur.

Port ve Soket Arasındaki Fark

PORT

- Sayısal bir tanımlayıcıdır (Örn: 443).
- Servisin konumunu belirtir.
- Aynı port üzerinden birden fazla bağlantı kurulabilir.

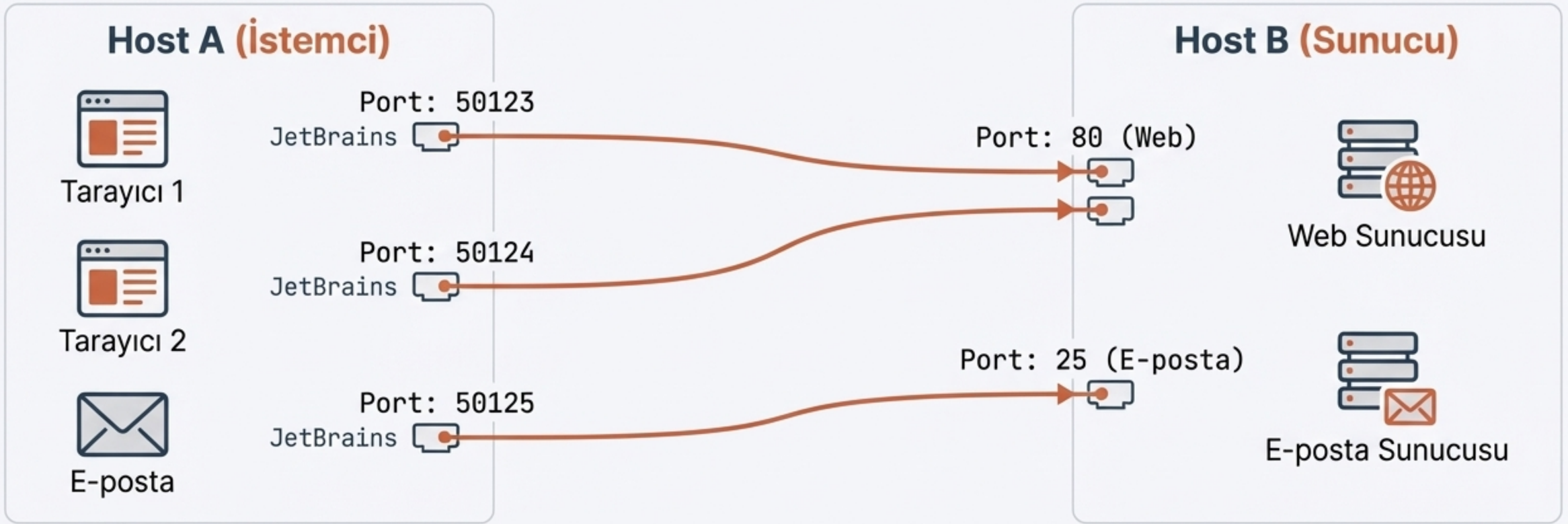


SOKET

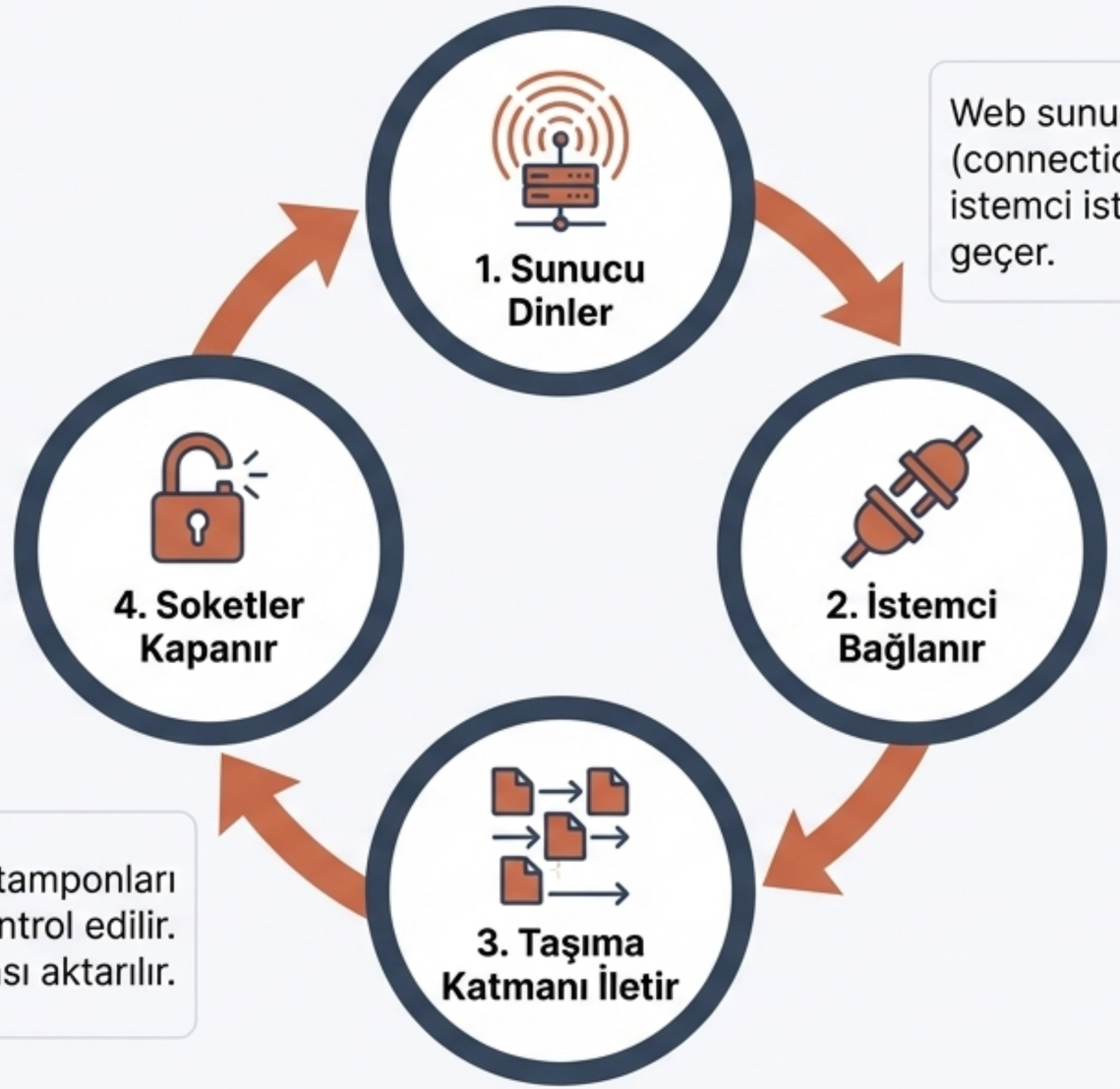
- İletişimin fiziksel uygulamasıdır.
- İşletim sisteminde Transmit (TX) ve Receive (RX) bellek tamponları (buffer) olarak fiziksel olarak uygulanır.
- Benzersiz bir bağlantıyı (Kaynak ve Hedef ikilisi) temsil eder.

Örnek: Soketler ile İletişim Ağı (Microchip Senaryosu)

- Bir istemci (Host A) aynı sunucuda (Host B) iki web sayfası ve bir e-posta işlemi başlatır.
- İşletim sistemi, her tarayıcı sekmesi ve e-posta istemcisi için farklı dinamik soket numaraları oluşturur.
- Sunucu (Host B), gelen talepleri ayırt etmek için hedef portlarını (80 ve 25) kullanır ve kendi tarafında bu bağlantılar için özel soketler açar.



Adım Adım TCP Bağlantı Süreci



Web sunucusu bir bağlantısız (connectionless) soket oluşturur ve istemci isteklerini dinleme moduna geçer.

İstemci kendi soketini oluşturur ve hedefe TCP bağlantı isteği gönderir. Sanal TCP bağlantısı "kuruldu" durumuna geçer.

TX ve RX bellek tamponları periyodik olarak kontrol edilir. Veriler soketler arası aktarılır.

İstemci onay (ACK) gönderir ve soketini kapatır. Sunucu onayı alır ve kendi soketini sonlandırır.

Berkeley Sockets API: Geliştirici Penceresi

1980'lerde UNIX için geliştirilen ve günümüzde endüstri standardı olan Soket Programlama arayüzü (API).

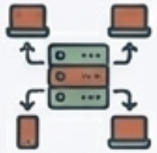
`socket()`
Yeni bir soket oluşturur.

`bind()`
(Sunucu tarafı) Soketi yerel IP ve Porta bağlar.

`connect()`
(İstemci tarafı) Sunucuya TCP/UDP bağlantısı kurar.

`send()` / `recv()`
Soket üzerinden veri gönderir ve alır.

En Çok Bilinen Portlar: Web ve Dosya Transferi

	**80 (TCP)**	**HTTP**	Şifresiz Web Trafiği
	**443 (TCP)**	**HTTPS**	Güvenli Web Trafiği (SSL/TLS)
	**20/21 (TCP)**	**FTP**	Dosya Transfer Protokolü
	**53 (TCP/UDP)**	**DNS**	Alan Adı Çözümleme (IP - İsim eşleştirme)
	**67/68 (UDP)**	**DHCP**	Otomatik IP Dağıtımı

En Çok Bilinen Portlar: E-posta ve Uzaktan Erişim

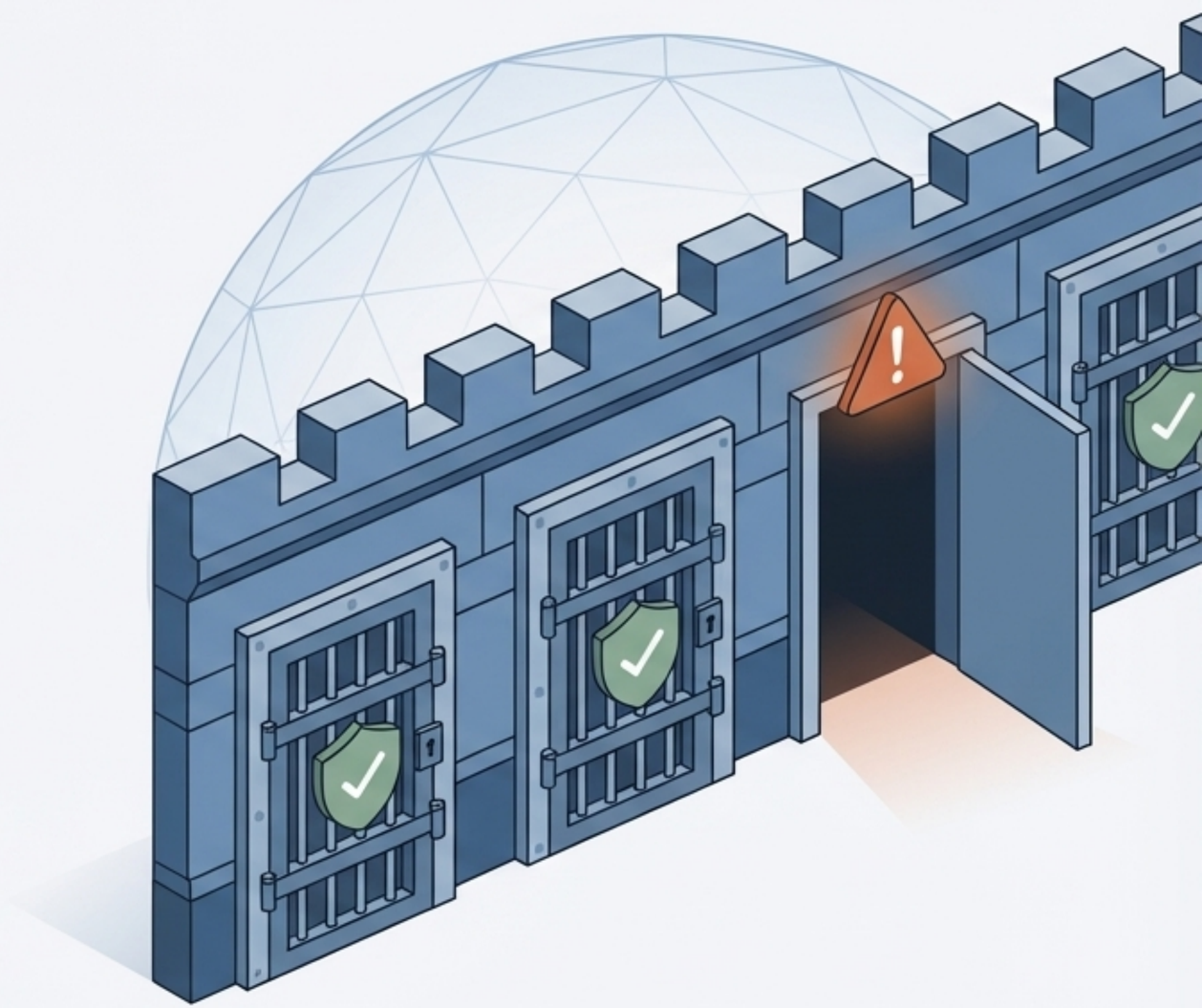
	**25 (TCP)**	**SMTP**	E-posta Gönderme
	**110/143 (TCP)**	**POP3/IMAP**	E-posta Alma (İstemciye indirme / Sunucuda okuma)
	**22 (TCP)**	**SSH**	Güvenli Uzaktan Bağlantı (Terminal)
	**23 (TCP)**	**Telnet**	Eski/Şifresiz Uzaktan Bağlantı
	**3389 (TCP)**	**RDP**	Windows Uzak Masaüstü Protokolü

Kritik Veritabanı ve Modern Sistem Portları

	**3306 (TCP)**	**MySQL**	Veritabanı Yönetimi
	**1433 (TCP)**	**MSSQL**	Microsoft SQL Server
	**27017 (TCP)**	**MongoDB**	NoSQL Veritabanı
	**6379 (TCP)**	**Redis**	Cache (Önbellek) Veritabanı
	**2375/2376 (TCP)**	**Docker**	Container API Yönetimi

Siber Güvenlikte Portların Önemi (Saldırı Yüzeyi)

- Portlar ağın **Saldırı Yüzeyini** (Attack Surface) belirler.
- **Servis Keşfi:** Açık portlar, sistemde hangi yazılımların çalıştığını ifşa eder (Örn: Port 22 açıksa SSH vardır).
- **Güvenlik Açıkları (Vulnerabilities):** Eski ve güncellenmemiş servisler doğrudan sisteme sızmak için kullanılır.
- **Network İzleme**: Anormal port trafiği (Örn: Port 4444) Botnet veya Command & Control bağlantılarına işaret eder.



Port Tarama ve Keşif (Reconnaissance)

Siber güvenlik uzmanları ve saldırganlar ağ haritasını çıkarmak için tarama araçları kullanır.

Nmap (En popüler), Masscan (Hızlı), Wireshark (Paket analizi).

Nmap Teknikleri

SYN Scan (-sS): Gizli tarama. IDS sistemlerinden kaçınmak için tam TCP bağlantısı kurmaz.

UDP Scan (-sU): DNS ve DHCP gibi bağlantısız protokolleri tespit eder.

Version Detection (-sV): Açık portun arkasındaki servisin sürümünü bulur.

```
user@host ~$ nmap -sS target.com

Starting Nmap 7.94...
Nmap scan report for target.com
Host is up (0.0023s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 1.24
seconds
```

Savunma ve Saldırı: Blue Team vs. Red Team

Red Team (Saldırı Taktikleri)

Hedef: Tespit edilmeden ağ keşfi ve zafiyet istismarı.

Taktikler: Stealth / Yavaş Tarama, Fragmented Packets, SSH/RDP Brute Force, Servis Exploitleri.

Blue Team (Savunma Taktikleri)

Hedef: Anormallikleri tespit etmek ve erişimi kısıtlamak.

Taktikler: Firewall Hardening (Sadece gerekli portları açma), IDS/IPS, Honeypot, SIEM (Ağ log analizi).