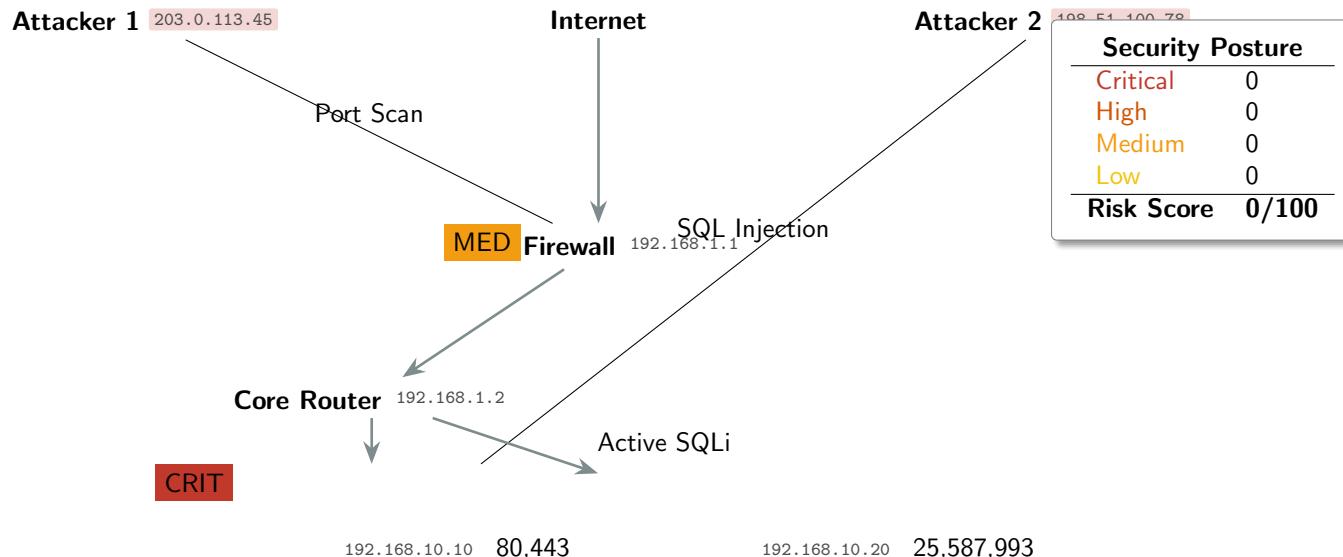server/.style
server/.style//
client/.style
client/.style//
router/.style
router/.style//
firewall/.style
firewall/.style//
switch/.style
switch/.style//
cloud/.style
cloud/.style//
attacker/.style
attacker/.style//
encrypted conn/.style
encrypted conn/.style//
suspicious conn/.style
suspicious conn/.style//
attack conn/.style
attack conn/.style//
bidirectional/.style
bidirectional/.style//
asset label/.style
asset label/.style//
threat label/.style
threat label/.style//
port label/.style
port label/.style//
[regular polygon, regular polygon sides=3, fill=, draw=!80, minimum size=cm, inner sep=0pt] at (1,2) ;
[font=, text=white] at (1,2) !;
[below, font=] at (1,2-0.15) 4;

Attacker 1 `203.0.113.45`　　**Internet**　　**Attacker 2** `198.51.100.78`

Port Scan

MED **Firewall** `192.168.1.1`　SQL Injection

Core Router `192.168.1.2`

Active SQLi

CRIT

`192.168.10.10` **80,443**　　　　`192.168.10.20` **25,587,993**

`CVE-2024-1234: 9.8` **1**　　**Mail Server**

HTTPS

Internal Firewall `192.168.1.3`

Core Switch `192.168.100.1`

App Server 1 `192.168.100.10` **App Server 2** `192.168.100.11` **DB Primary** `192.168.200.10`

TLS 1.3　　TLS 1.3

Unauthorized Access　　Replication

Ransomware

WS-001 `192.168.100.` CRIT **02** `168.100.` **WS-003** `192.168.100.52`　　**DB Replica** `192.168.200.11`

Security Posture	
Critical	0
High	0
Medium	0
Low	0
Risk Score	**0/100**

Legend
→ **Normal**
— **Encrypted**
— **Suspicious**
— **Attack**

Generated: November 16, 2025 Network Diagram v1.0 Scale: 1.0x