Time Analysis of Incident

Recon

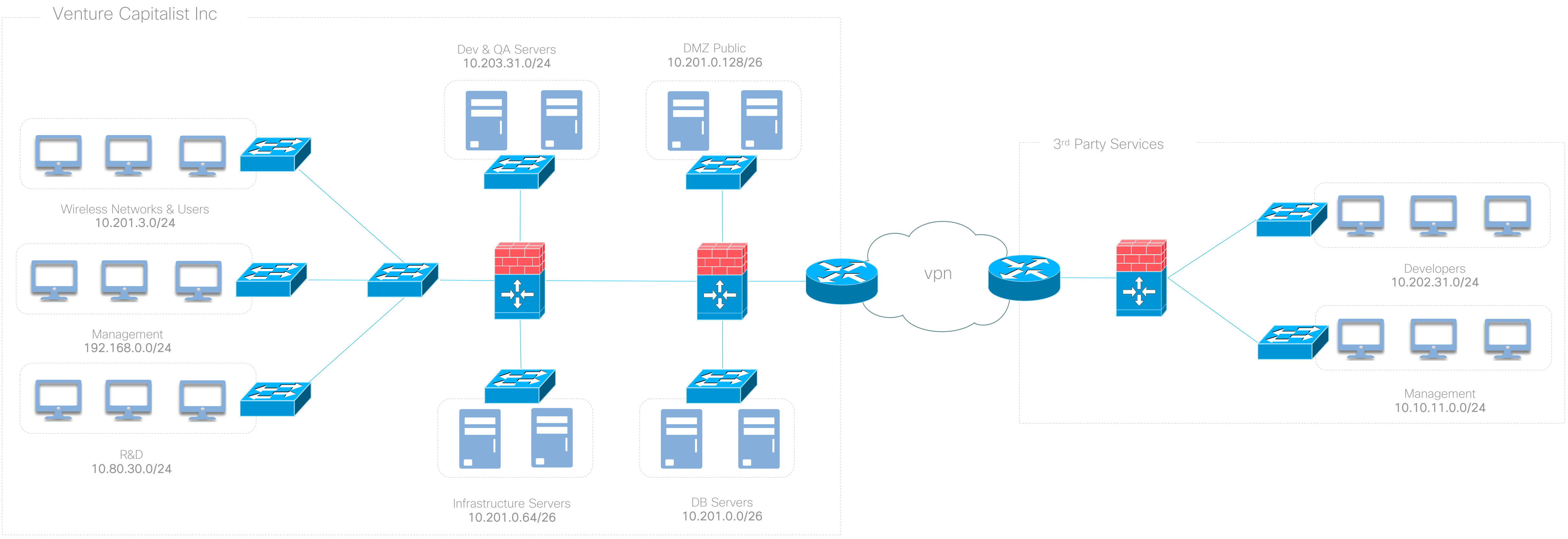
Initial Access

C2

Lateral

Exfil

Network Diagram



C2 Beacon Activity

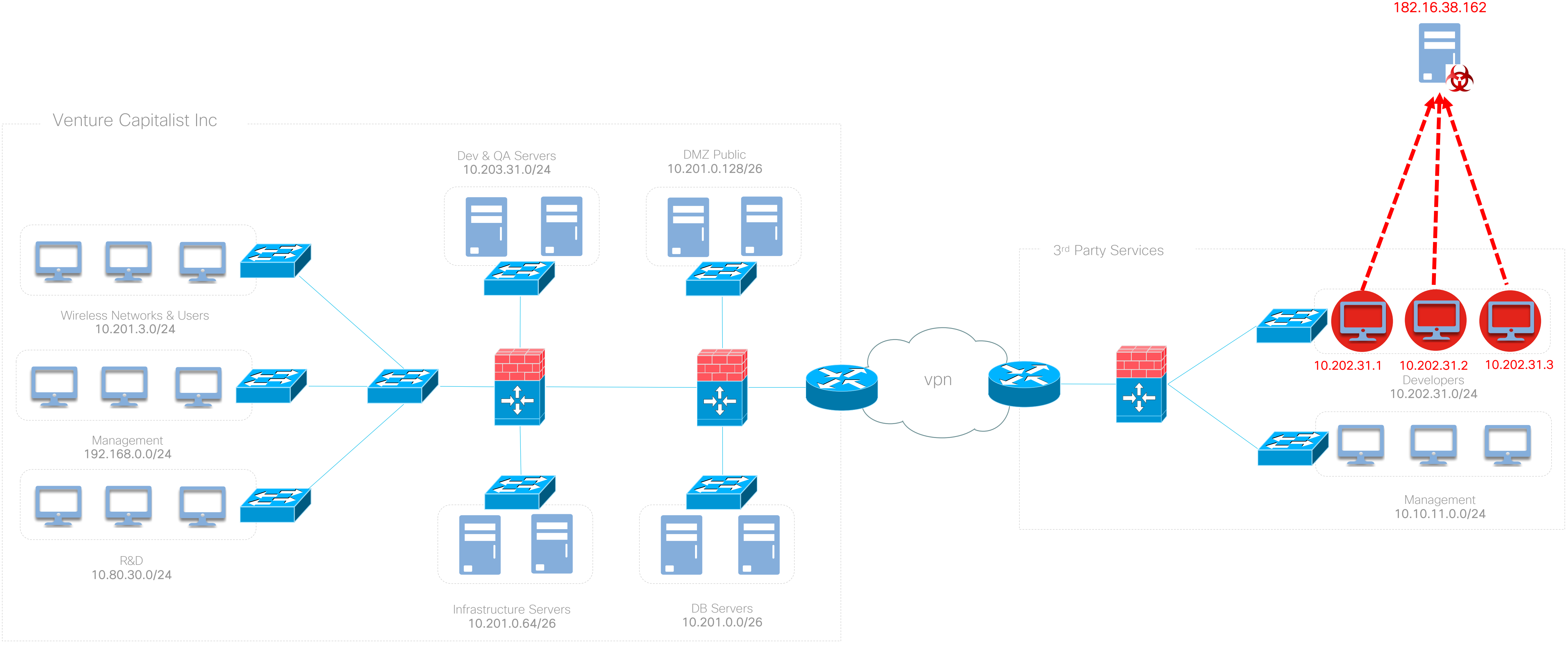
Recon

Initial Access

C2

Lateral

Exfil



Download of multiple file types

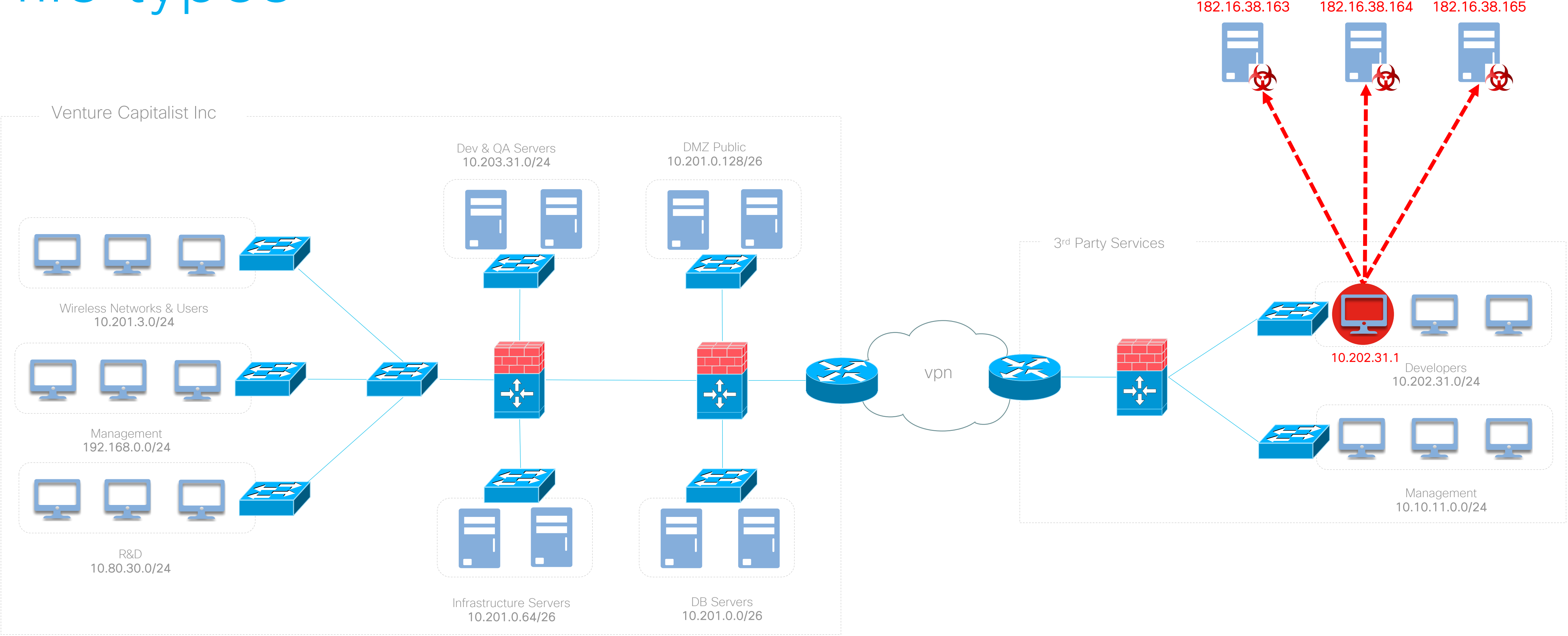
Recon

Initial Access

C2

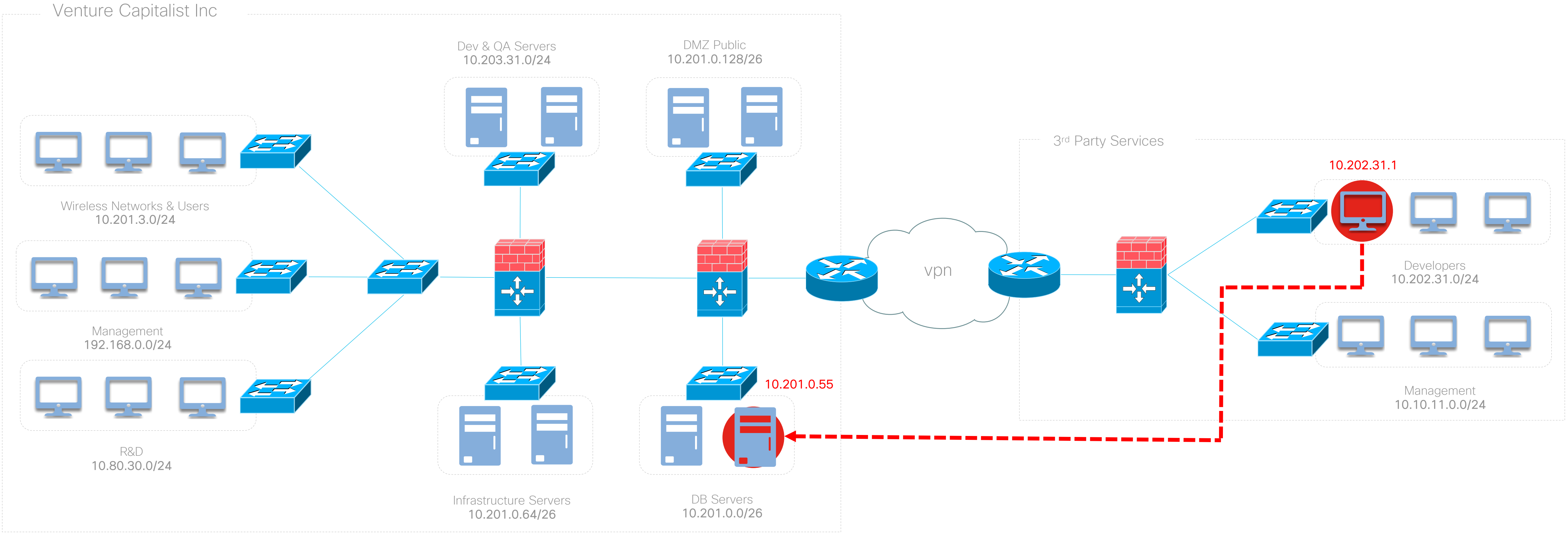
Lateral

Exfil



SQL Injection

Recon · Initial Access · C2 · Lateral · Exfil



SSH Upload

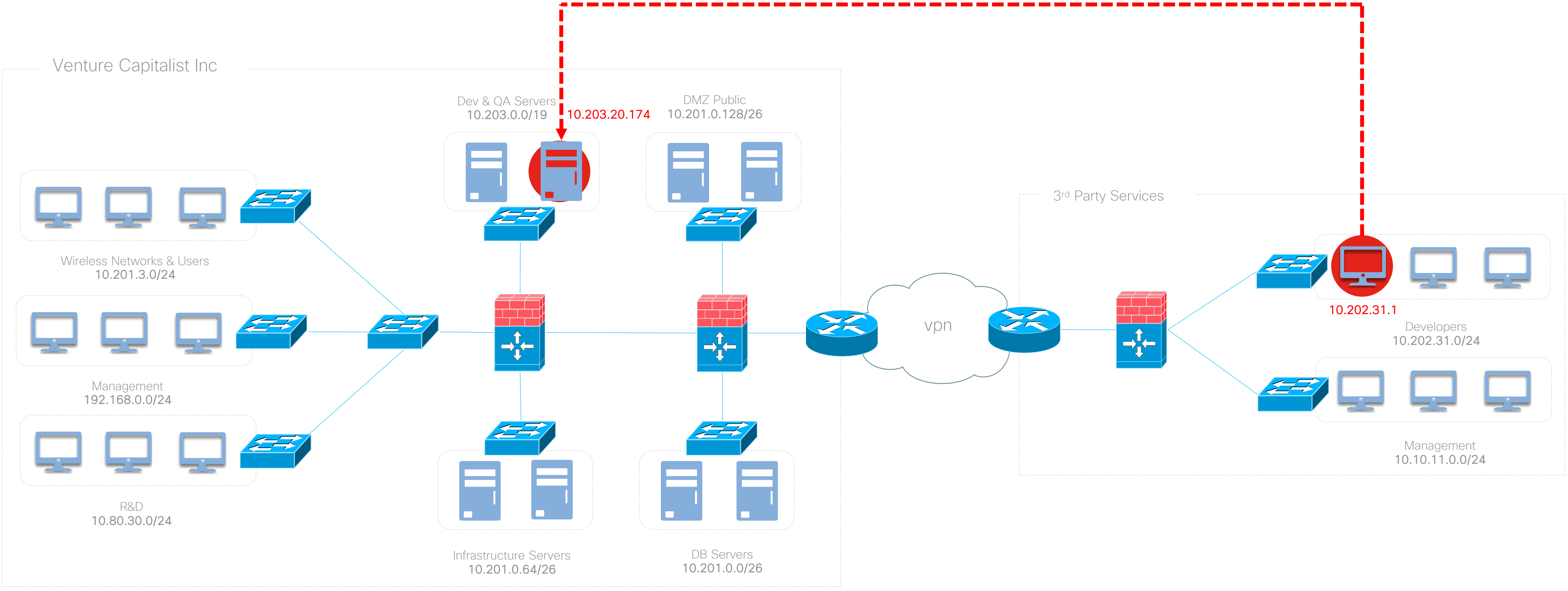
Recon

Initial Access

C2

Lateral

Exfil



Scheduled File Transfer over ICMP Tunnel

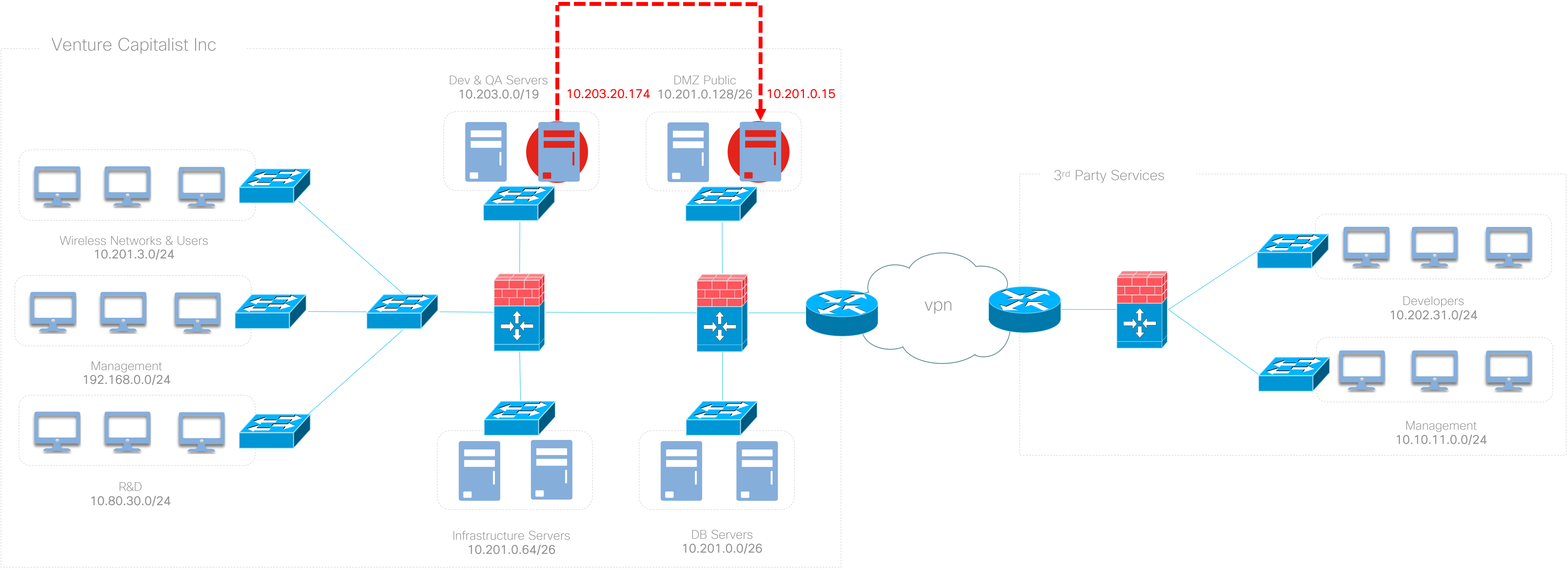
Recon

Initial Access

C2

Lateral

Exfil



Exfiltration over Custom Protocol

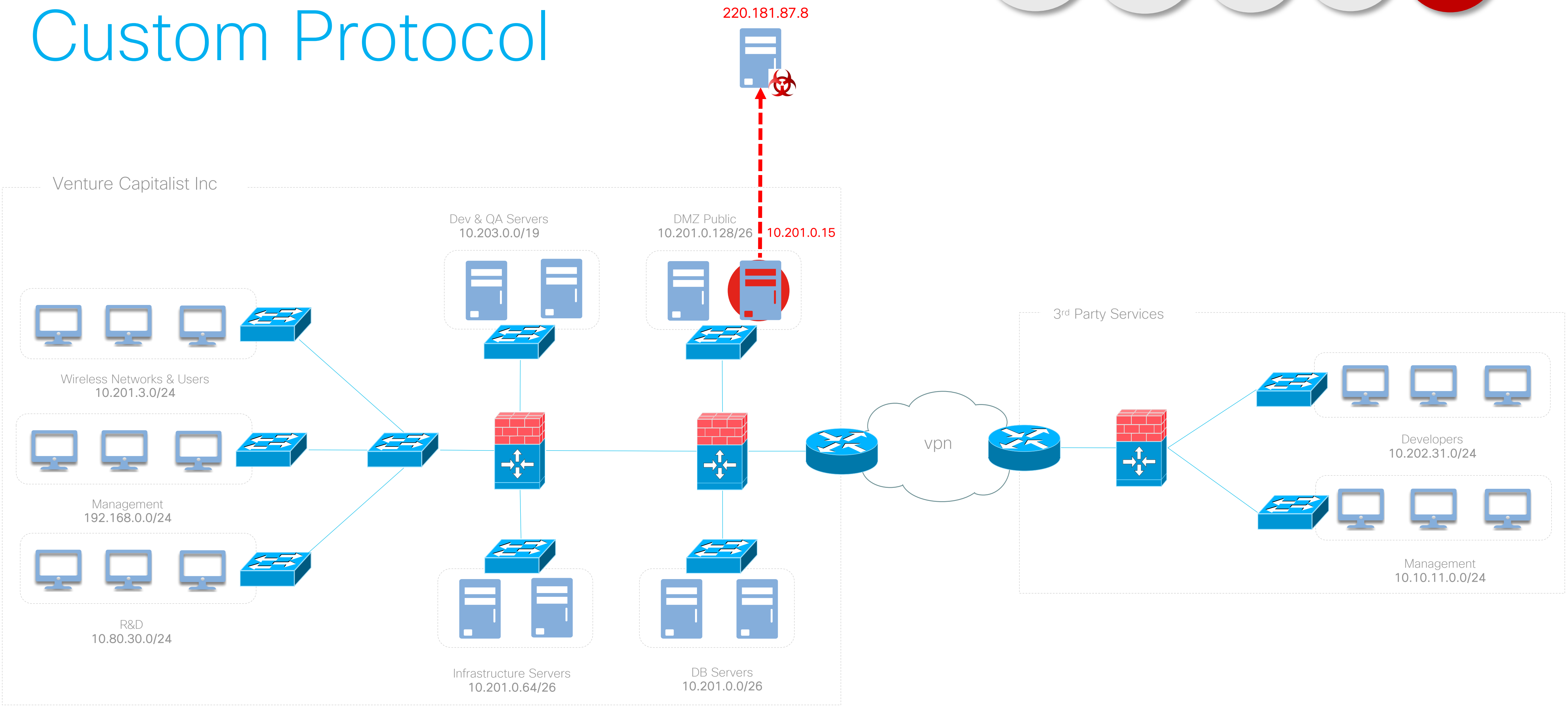
Recon

Initial Access

C2

Lateral

Exfil



Time Analysis

Time	Activity
11:50 am	Compromised internal hosts beaconing to C2 infrastructure (probably pre-acquisition).
12:22 pm	C2 instructs internal host to download suspicious file extensions from different locations with the objective to bypass security controls (ex: blocking of exec files)
12:22 pm	Compromised hosts performs SQL Injection on internal web application (credential dump, credit card info dump)
12:24 pm	Internal host communicates over SSH to a QA server and performs an upload.
12:29 pm	ICMP tunneling technique used to move credit card data from QA server to staging server in DMZ using scheduled transfers
12:57 pm	Staging server in DMZ exfiltrates data over custom protocol to known Talos' Blacklist IP Address