Cloudflare Spectrum

Layer 4 TCP/UDP Protection for Non-HTTP Traffic

Enterprise Sales Training • Brandon Crowe

What Is Spectrum?

- Layer 4 reverse proxy that extends Cloudflare's DDoS protection to any TCP/UDP protocol
- Protects non-HTTP traffic: SSH, RDP, databases, game servers, IoT, email, VPN, FTP
- Origin IP masking — attackers can't find or target your real server
- L4 DDoS protection — volumetric attacks absorbed across 330+ Cloudflare cities
- No agents or software required — just DNS change + Spectrum configuration
- Priced by concurrent connections — active simultaneous sessions, not total traffic

Why Spectrum Matters (The Business Case)

- Cloudflare protects HTTP/HTTPS traffic with WAF, CDN, and DDoS protection — but not everything is HTTP
- SSH, RDP, databases, game servers, IoT devices — all run on TCP/UDP and are exposed by default
- Without Spectrum, origin server IPs are publicly visible and directly attackable
- A single volumetric DDoS attack can take down a game server, bastion host, or production database
- Spectrum hides the origin behind Cloudflare's anycast network — the same infrastructure that protects 20% of the web
- Enterprise feature — positions alongside WAF, API Shield, and Magic Transit in security conversations

How Spectrum Works — The Traffic Flow

1. **Client connects — to ssh.example.com:22 (or any configured subdomain + port)**
2. **DNS resolves — to Cloudflare's anycast IP, not the origin server**
3. **Edge accepts — Spectrum proxy accepts the TCP/UDP connection at the nearest POP**
4. **DDoS filtering — L4 inspection: SYN flood mitigation, volumetric attack absorption, connection tracking**
5. **Traffic forwarded — clean connections proxied to origin server at the real IP + port**
6. **Origin sees CF IP — server only sees Cloudflare's IP as the source, real client IP hidden**

7. Analytics — Dashboard shows concurrent connections, bytes ingress/egress, protocol stats

Supported Protocols & Common Ports

Protocol	Port(s)	Use Case
SSH	22	Remote server access, bastion hosts
RDP	3389	Windows Remote Desktop
MySQL	3306	Database connections
PostgreSQL	5432	Database connections
Redis	6379	Cache / data store
Minecraft	25565	Game server (TCP)
SMTP	25 / 587	Email (outbound)
IMAP / POP3	993 / 995	Email (inbound)
MQTT	1883	IoT messaging
Custom TCP/UDP	Any	VPN, SCADA, proprietary protocols

Real-World Use Cases

Gaming (Minecraft, Rust, ARK, CS2) — The #1 Spectrum use case. Game servers expose public IPs to every player. A single malicious player with a DDoS booter ($5-20) can knock 1000 players offline. Spectrum hides the origin IP behind Cloudflare's anycast network. Players connect to play.example.com, volumetric attacks get absorbed at the edge, and the server stays online. Minecraft server operators are the largest user base for Spectrum.

SSH & Bastion Hosts — Enterprises run jump boxes as gateways to internal infrastructure. The bastion's IP must be publicly accessible, making it a target for brute-force attacks and DDoS. Spectrum proxies SSH traffic so the bastion only accepts connections from Cloudflare's IP ranges. Origin IP stays hidden. DDoS absorbed at the edge.

Production Databases — MySQL, PostgreSQL, Redis, MongoDB exposed to the internet get attacked constantly. Port scanners find them within minutes. Spectrum adds a protection layer — origin IP hidden, L4 DDoS filtering, connection rate limiting at the edge.

RDP (Windows Remote Desktop) — Port 3389 is one of the most exploited protocols on the internet. Attackers scan for open RDP ports and run credential-stuffing attacks. Spectrum proxies RDP connections, hiding the Windows server behind Cloudflare.

IoT & Industrial Control Systems — MQTT brokers, SCADA systems, and sensor networks need internet connectivity but can't install agents on every device. Spectrum protects the broker/controller without touching the devices. Critical for manufacturing, utilities, and smart building infrastructure.

Email Servers — SMTP, IMAP, POP3 servers are frequent DDoS targets. Spectrum proxies mail traffic so the mail server IP stays hidden. Volumetric attacks absorbed at the edge.

What I Built — Spectrum on saltwaterbrc.com

- Created DigitalOcean VPS (Ubuntu 24.04, $6/mo) as SSH origin server
- Configured Spectrum app: ssh.saltwaterbrc.com > TCP/22 > origin:22
- Tested SSH through Spectrum — server sees Cloudflare IP (104.28.x.x), not real client IP
- Origin IP masking confirmed — attacker cannot discover the real server
- Firewall lockdown: UFW rules allow SSH only from Cloudflare's 15 IPv4 CIDR ranges
- Direct SSH to origin IP is blocked — only ssh.saltwaterbrc.com works
- Spectrum Analytics live in dashboard: concurrent connections, ingress, egress

Live Demo — Terminal Commands

Connect through Spectrum (proxied through Cloudflare):

```
ssh root@ssh.saltwaterbrc.com
```

Server sees Cloudflare's IP as the source — your real IP is hidden.

Verify origin IP masking:

```
who -a
```

Shows login sessions — source IP will be 104.28.x.x (Cloudflare), not your real IP.

Direct SSH to origin (blocked after firewall lockdown):

```
ssh root@<origin-ip>
```

Connection times out. Firewall only allows Cloudflare IP ranges.

Origin Firewall Lockdown — Cloudflare IPs Only

The critical security step. Restrict SSH access to Cloudflare's IP ranges so direct access is blocked:

```
ufw allow from 173.245.48.0/20 to any port 22
ufw allow from 103.21.244.0/22 to any port 22
ufw allow from 141.101.64.0/18 to any port 22
ufw allow from 108.162.192.0/18 to any port 22
ufw allow from 198.41.128.0/17 to any port 22
ufw allow from 162.158.0.0/15 to any port 22
ufw allow from 104.16.0.0/13 to any port 22
ufw allow from 172.64.0.0/13 to any port 22
```

... + 7 more Cloudflare ranges (see cloudflare.com/ips)

```
ufw default deny incoming && ufw default allow outgoing && ufw enable
```

Where Spectrum Fits — Cloudflare Security Layers

Layer	Product	Protects
L7 (HTTP/HTTPS)	WAF, API Shield, Bot Management	Web applications, APIs, forms
L4 (TCP/UDP)	Spectrum	SSH, RDP, databases, games, IoT, email

L3/L2 (Network)	Magic Transit, Magic WAN	Entire network ranges, BGP-level DDoS protection

Pricing Model

- Spectrum is priced per concurrent connection — how many active sessions at the same time
- NOT priced by bandwidth — a game server with 1000 concurrent players costs the same whether they transfer 1 GB or 100 GB
- Enterprise feature — available on ENT plans, often bundled with other security products
- Free trial available for evaluation on existing zones

Sales Talking Points

- "Cloudflare protects your web traffic — but what about SSH, RDP, databases, game servers? That's Spectrum."
- "Spectrum hides your origin IP. Attackers can't find it, can't scan it, can't DDoS it directly."
- "No agents, no VPN, no complexity. DNS change + Spectrum config. That's the entire deployment."
- "Minecraft server operators are our biggest Spectrum customers. One DDoS attack costs them thousands in lost revenue."
- "I set this up on my own infrastructure in 30 minutes. I can show you it working in terminal right now."