Email Routing Refactor (ERR)

Initiative Summary
DCSS, October 2020

ERR Overview

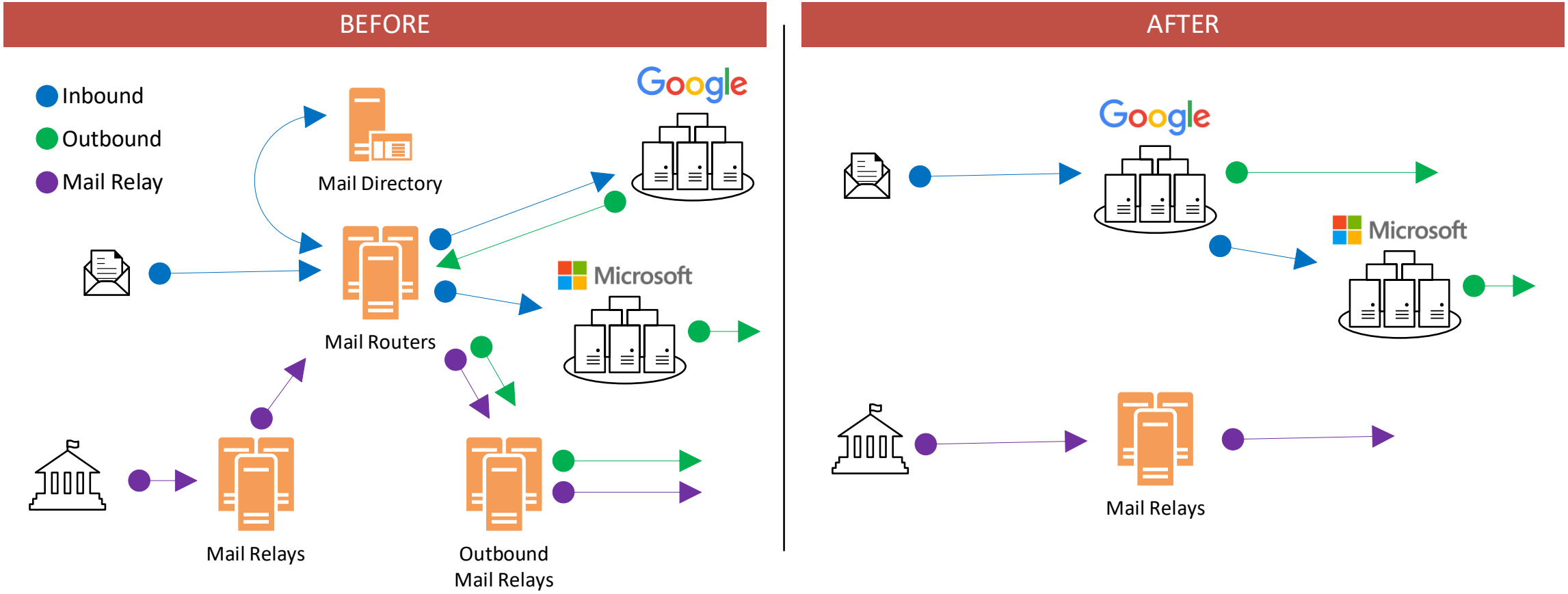
ERR migrated the Virginia Tech email routing services from on-premise hardware to the cloud solutions provided by Google and Microsoft.

The initiative involved changing the routing for over 350,000 vt.edu email objects including user email addresses, aliases, Google groups, GAEs, service accounts and resource accounts. The university's total email volume represents nearly 1 billion total inbound/outbound messages per year.

The initiative provides university's email communication with the following benefits

- Improved scalability and reliability
- Enhanced security
- Better standards compliancy
- Better spam and phishing mitigation
- Lower costs—less on-prem hardware & software to purchase, maintain, service
- Easier administration
- Fewer points of failure
- Better troubleshooting & support

ERR Overview



ERR Deployment Phases

- Phase 1: smtp.vt.edu to Google
  - Completed: 7/15
  - Communications: 6/25*, 7/1, 714
  - Incident Tickets: 23
- Phase 2: FE accounts to Google Groups
  - Completed: 7/24
  - Communications: 6/25*, 7/1, 7/17, 7/24
  - Incident Tickets: 3
  - Follow-up Work: Data lists published 8/6 and 8/12
- Phase 3: Elimination of Campus Return Trip
  - Completed: 7/29
  - Communications: 6/25*, 7/1, 7/28, 7/29
  - Incident Tickets: 0
- Phase 4: MX points to Google
  - Completed: 8/1
  - Communications: 6/25*, 7/1, 7/30, 8/1
  - Incident Tickets: 0

* ITC Working Group

ERR Benefits

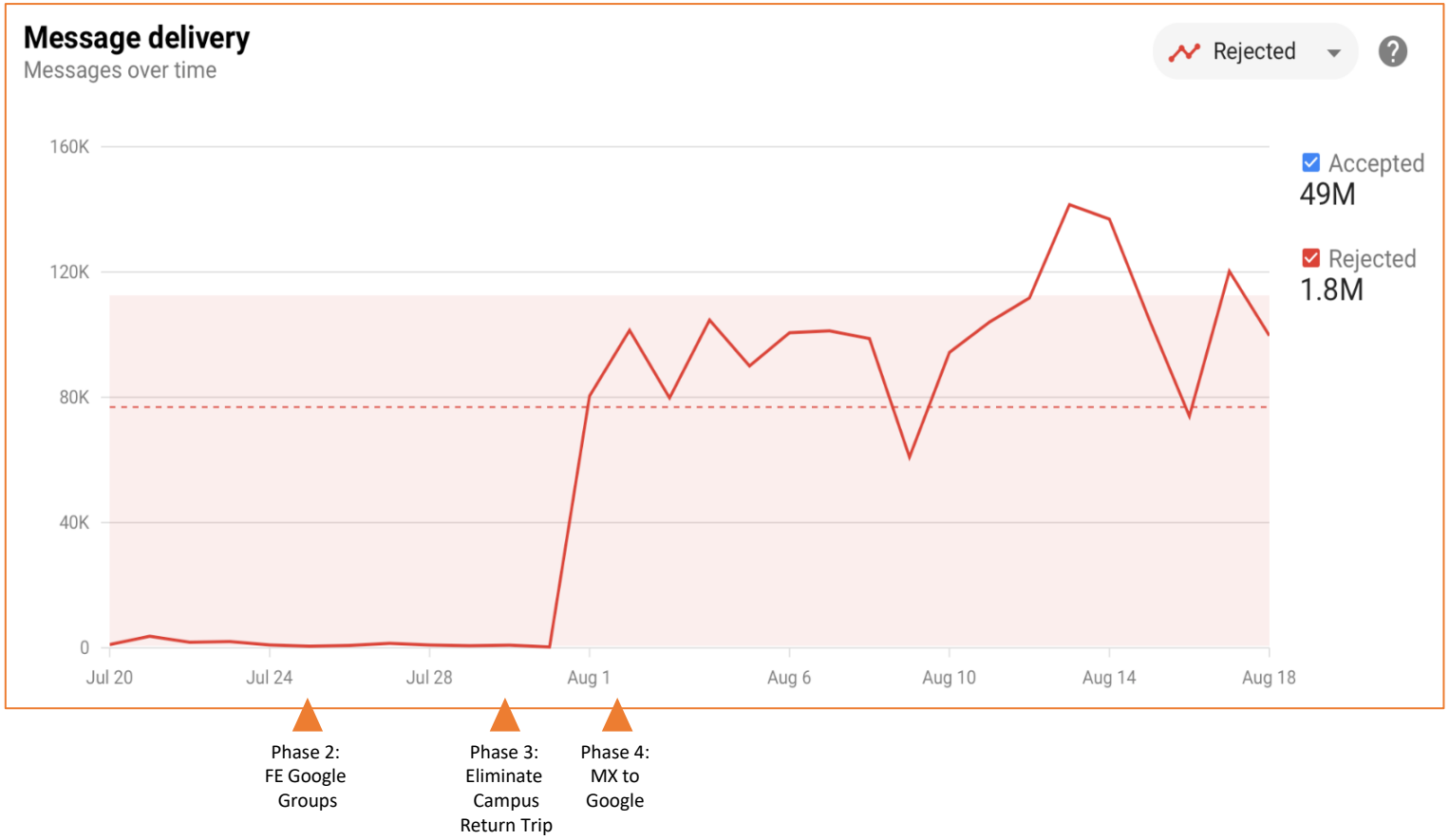
Google: Spam/Phishing Message Rejection

Google is managing spam and phishing protections instead of static and infrequently updated on-prem lists resulting in

- More accurate spam labeling
- Prevention of known spam and phishing senders from reaching users mailboxes

Daily Spam/Phishing Message Rejection

- Before ERR: 500 - 2,000
- After ERR: 100,000 - 200,000



Google: Spam/Phishing Message Rejection

Sept. 12 through Oct. 12 data

Daily Spam/Phishing Message Rejection

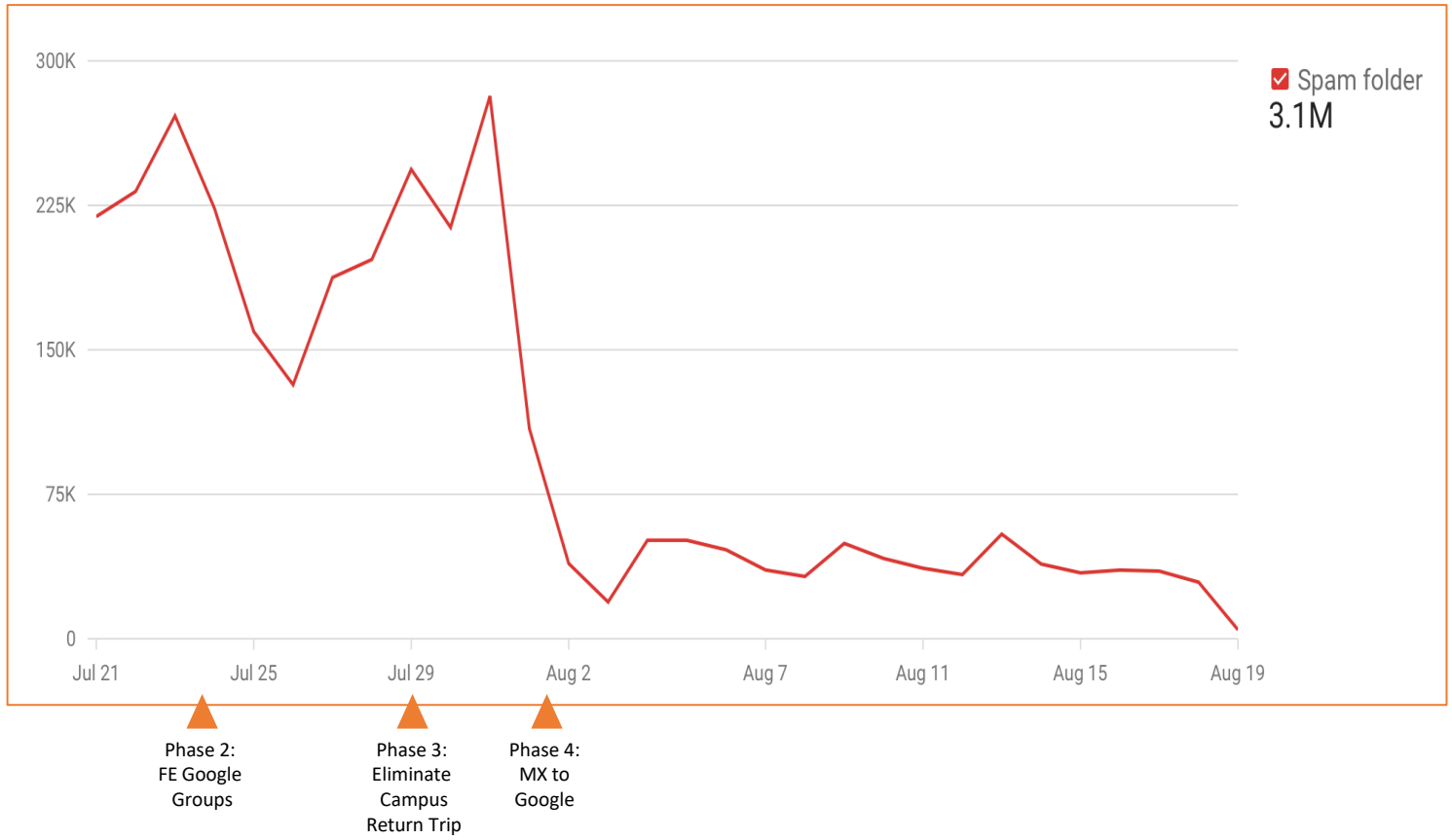
- Before ERR: 500 - 2,000
- After ERR: 100,000 - 200,000+

Google: Phishes Reaching User Mailboxes

Due to Google's increased rejection of phishing messages, VT users are seeing significantly less phishes reach their spam folders.

Daily messages being sent to spam folders

- Before ERR: 135,000 - 275,000
- After ERR: 5,000 - 25,000

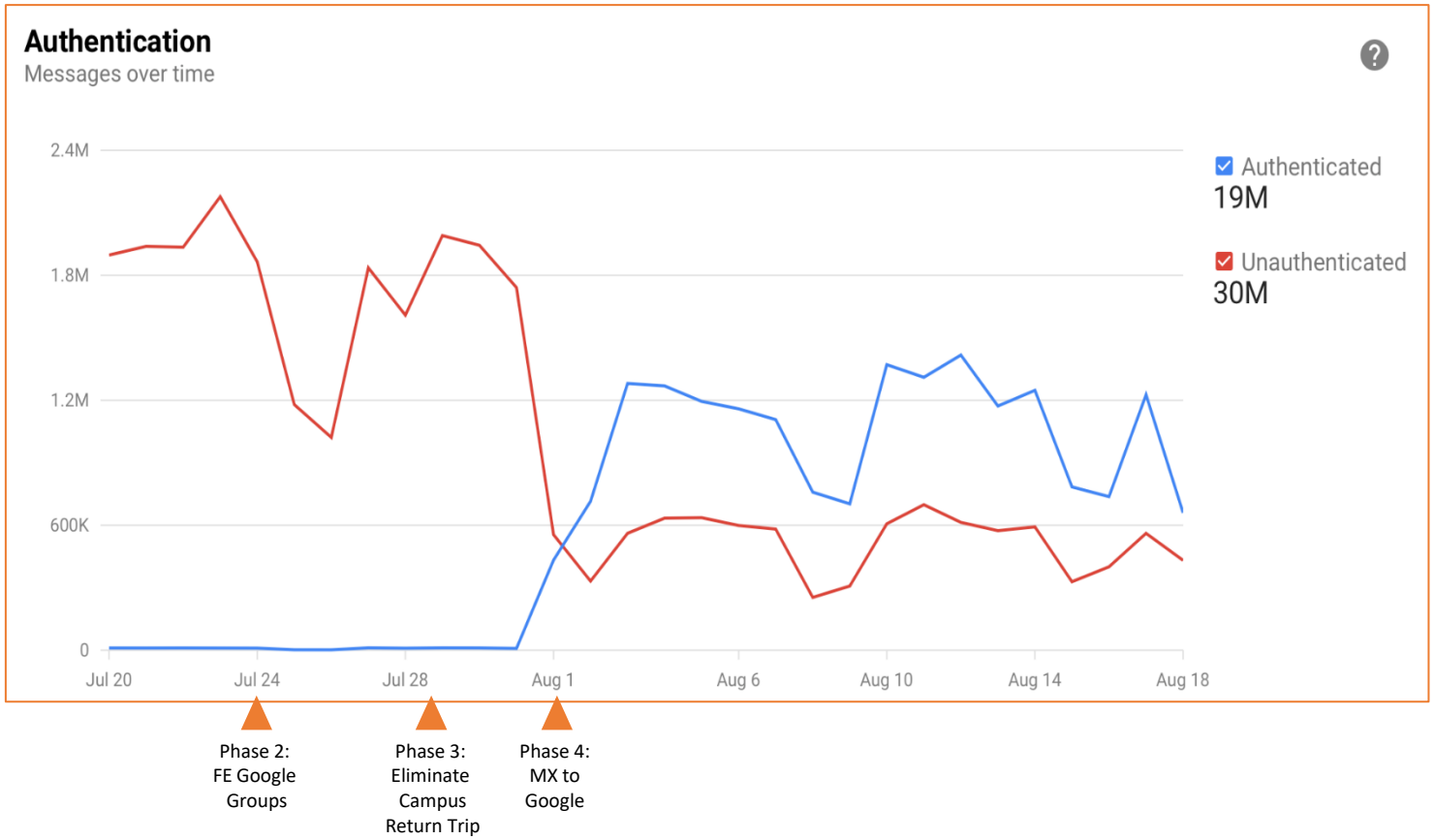


Google: Inbound Authentication Enforcement

Google is able to enforce DMARC, DKIM, and SPF authentication standards providing better protection against spam and phishing senders.

With ~60+ million monthly Virginia Tech emails, Google is seeing DMARC compliancy at

- Before ERR: less than 1%
- After ERR: ~64% (last 31 days; 38M of 59M pass DMARC)

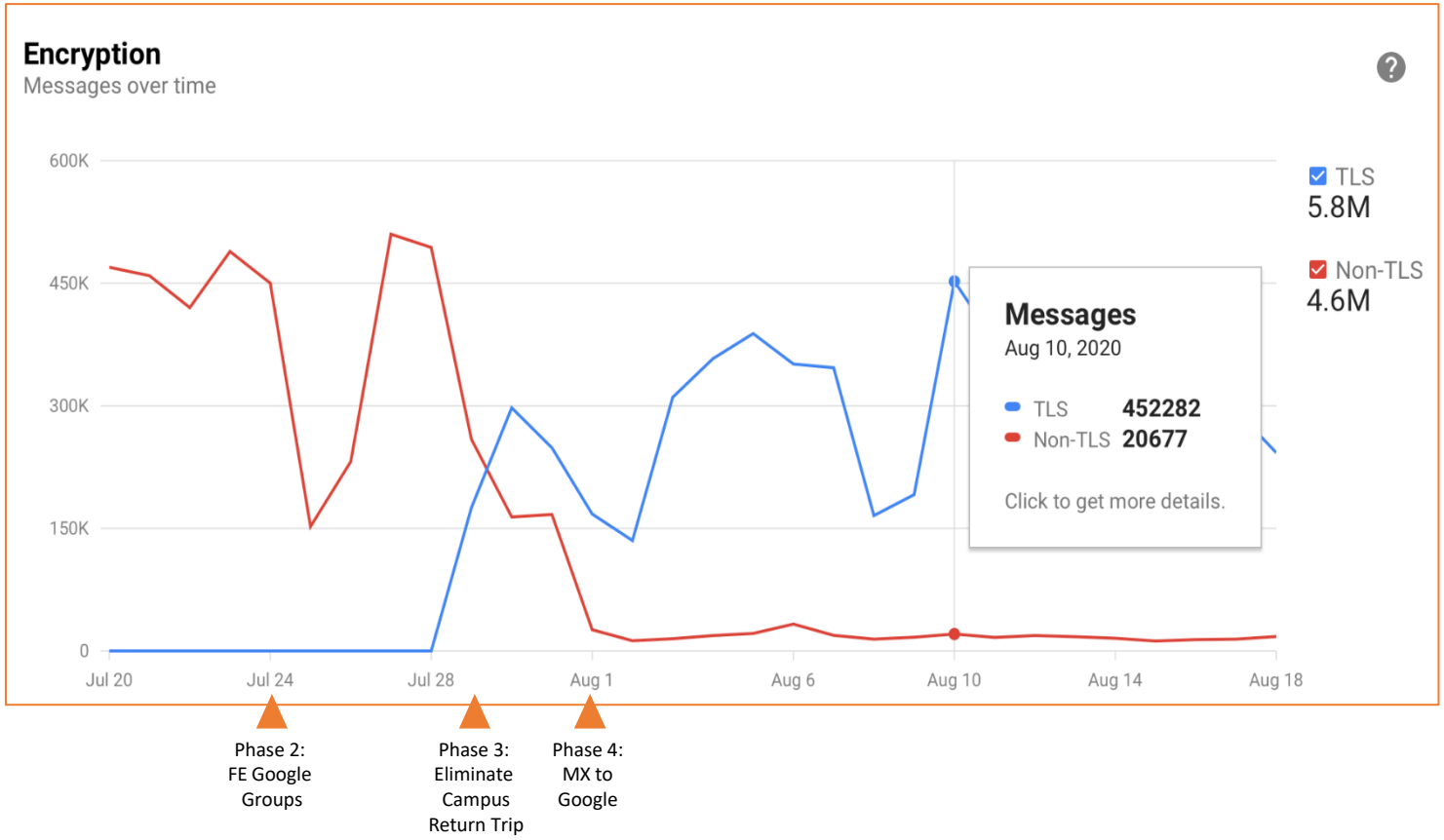


Google: TLS Encryption

Google is enabling TLS encryption on outbound messages to recipient hosts.

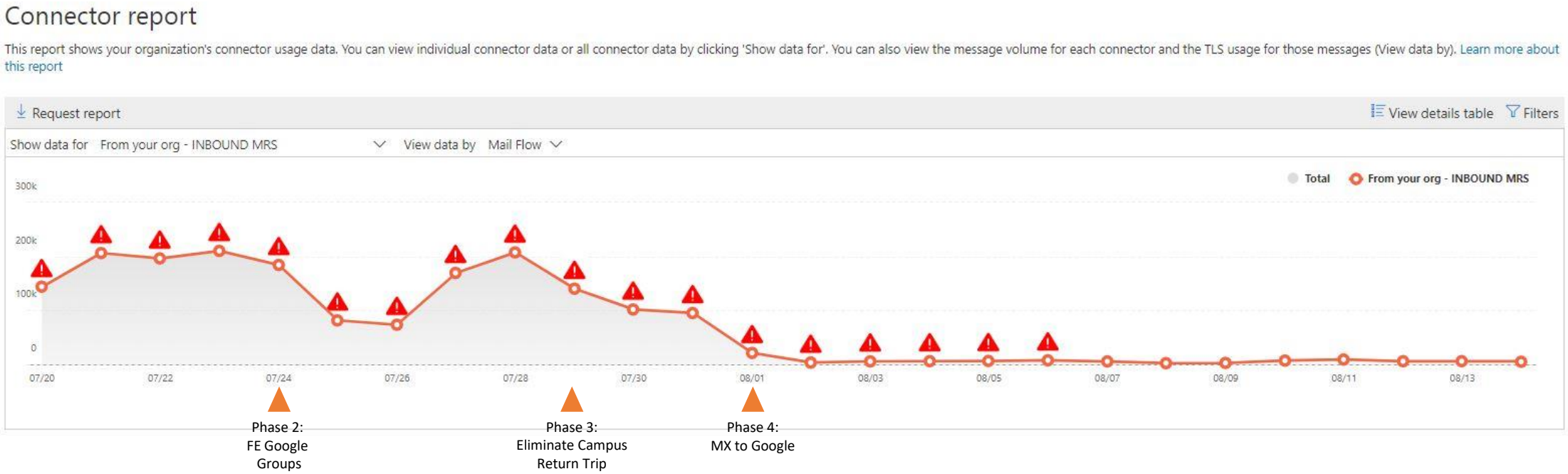
With ~10+ million outbound monthly Virginia Tech emails, Google is seeing TLS encryption at

- Before ERR: 0%
- After ERR: ~95%

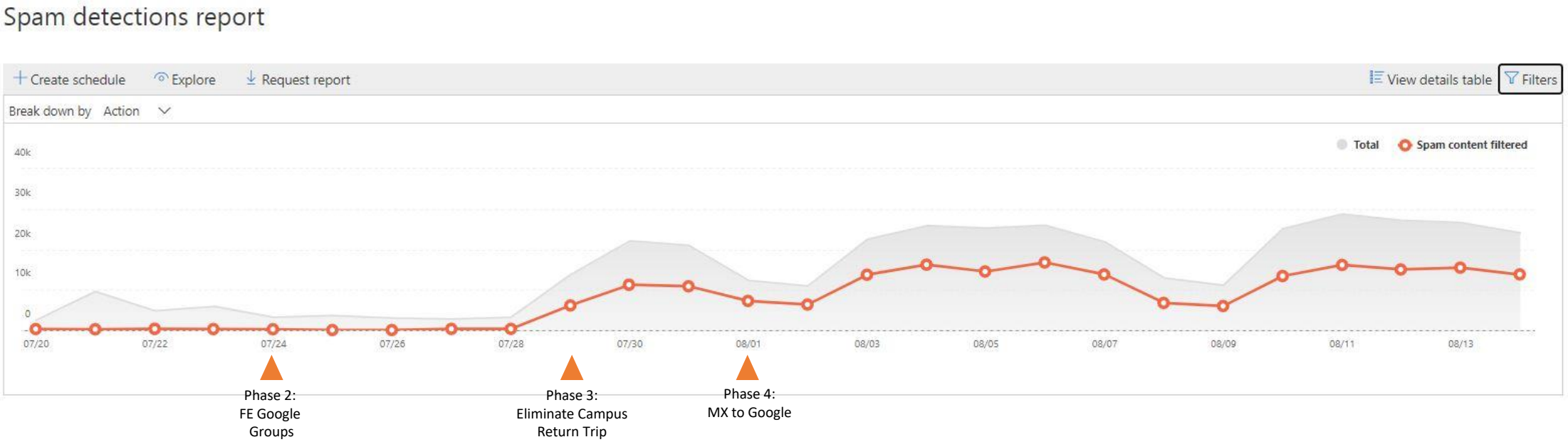


EO: Connector Traffic Elimination

With the on-premise solution, Virginia Tech was required to use an Exchange Online Connector to trust all traffic from the VT Mail Routers. With ERR, traffic across this connection has been nearly eliminated resulting in most emails delivered to Exchange Online mailboxes being scanned and protected by both Google Gmail spam/phishing rules and Microsoft's Exchange Online Protection and Advanced Threat Protection solutions.



EO: Spam Detections

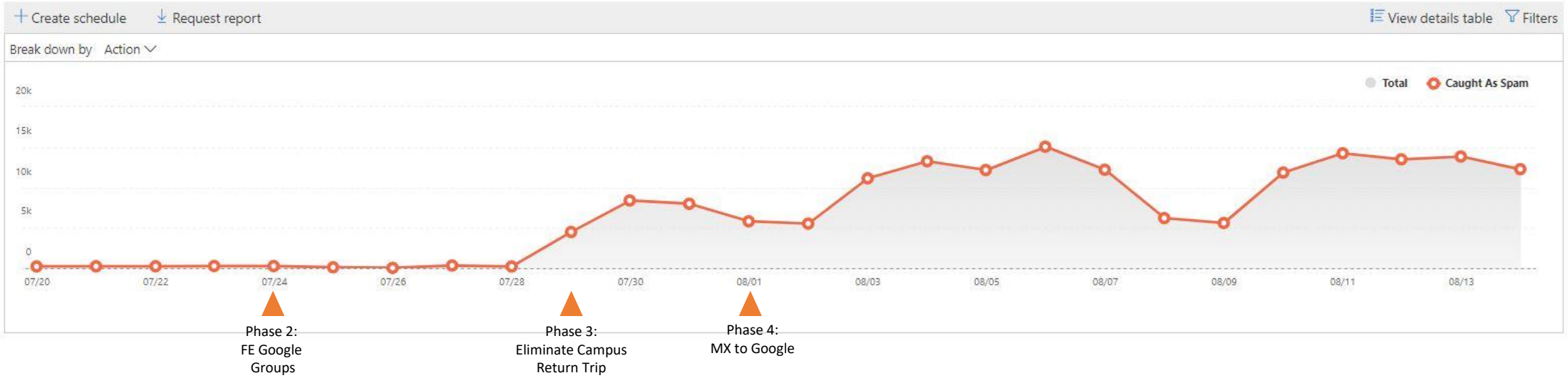


With ~300,000 daily Exchange Online emails received by VT users, spam detection and filtering improvements are

- Before ERR: ~0 to ~5,000 daily messages
- After ERR: ~7,000 to ~24,000 daily messages

EO: Spoofing Protection

Spoof Mail Report



With ~300,000 daily Exchange Online emails received by VT users, spoofing prevention improvements are

- Before ERR: 0 daily messages
- After ERR: 5,000 to 15,000 daily messages

ERR Clean Up

- There is still work to be done.
- Planned work includes
  - Migrate the remaining on-premise Mail Relay Services (mailrelay.smtp.vt.edu) to the new Outbound Mail Relays (OMRs) built by NI&S
  - Decommission legacy on-premise Mail Routers (6), Mail Relays (2), Logstash Server (1), and the Mail Directory Cluster (2)
  - Decommission the LDAP push from Middleware to the legacy Mail Directory Cluster
  - Investigate possible process improvements relating to FE Google Groups

Discussion