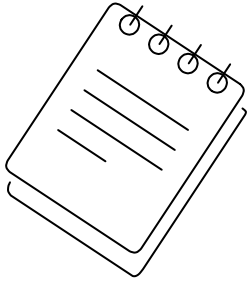




GlobalProtect Remote Access VPN



GlobalProtect™



What we'll explore today

- 1 What is the Enterprise Firewall Service?
- 2 GlobalProtect VPN Basics
What, why, when, who, and how
- 3 How we can help you prepare
- 4 How to get help
- 5 Closing Q & A



1

What is the Enterprise Firewall Service?

Cloud
Firewall

Border
Firewall

Data
Center
Firewall

VPN



Quick Project History

- Emerged from the Enterprise Firewall Project
- Scheduled to engage units late Spring 2020
- Pandemic = Teach and Work Remote
- OIS Security Needs
- Accelerated Timeline



2 — The GlobalProtect VPN Basics —

What • Why • When • Who • How



WHAT

Infrastructure



Network Topology

Next-Gen VPN Technology • Network Traffic

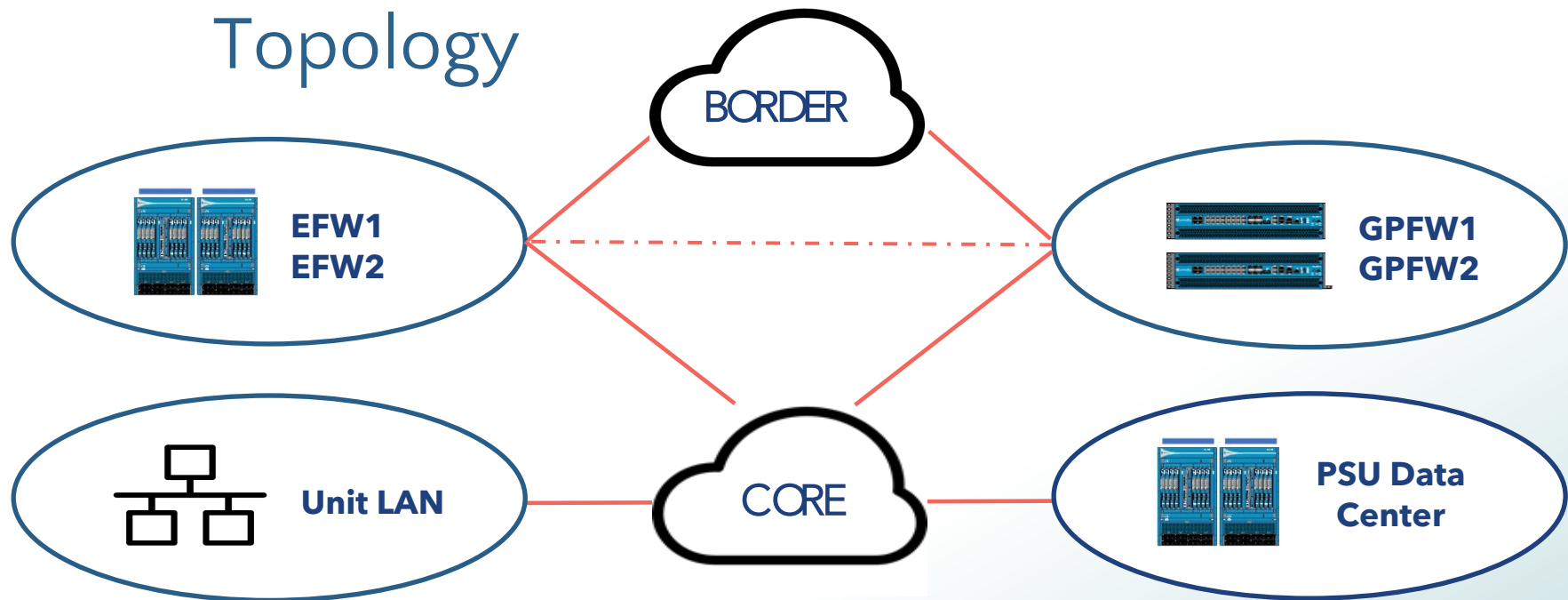
High Availability • Performance



Infrastructure



Topology





Infrastructure



Next-Gen VPN Technology

- Anti-Virus
- O-day Analysis
- Anti-spyware
- Application enforcement
- Vulnerability Protection
- EAD User/Group enforcement



Infrastructure



Network Traffic

- Full-tunnel
- Internet access enforced at the EFW
- Familiar experience as when on campus



Infrastructure



High Availability

- On-premise hardware appliances in parallel to Border Firewall
- Active/Passive Cluster
- Near hitless sub-second failover



Infrastructure



Performance

- Supports 10s of Gbps VPN throughput
- Supports 10s of thousands concurrent users
- Scalable design and architecture



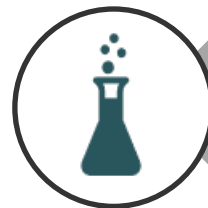
WHY



Secure Connections



Secure People



Secure Resources



Secure Connections

Pre-logon VPN • Single Sign-On Access • HIP



Secure Connections

Pre-logon VPN

- VPN connected before user logs in to their system
- Available only for Windows and macOS
- Remote system administration
- Remote EAD authentication



Secure Connections

Single Sign-On

- Uses the familiar Web Access and Azure AD Single Sign-On
- Provides Two-Factor Authentication
- EAD userID to IP address mappings for authorization



Secure Connections



Access

- Role-based gateways (external v. internal)
- Different access for Faculty & Staff, Students, and Contractors
- Access is managed by unit defined EAD security groups.
- EAD userID and groups used for authorization
- HIP (Host Information Profile)



Secure Connections

Host Information Profile (HIP)

- Worked with OIS on requirements
- Level 1/2 access
- Level 3/4 access



Secure Connections

Host Information Profile (HIP) for Level 1&2

- Must have supported Operating System
- Must have antivirus with Real Time Protection (RTP)
- Must have signatures updated within the past 30 days
- Must have a supported GlobalProtect Agent



Secure Connections

Host Information Profile (HIP) for Level 3&4

- Must meet all requirements for Level 1&2
- Must also have Splunk agent
- Must also have Nessus agent
- Must also have Cylance anti-malware agent must be installed, RTP enabled, and antivirus definitions less than 30 days old



Secure Connections

Host Information Profile (HIP) Challenges

- PSU doesn't yet have a standard anti-malware
- Some enclaves are impossible to enforce L3&4 HIP -- Lionpath, SIMBA, etc
- Personal machine use



Clientless VPN



- Encouraged for personal machine use
- No client installation needed
- Uses HTML5
- Leverages F&BIT RDS cluster
- Replaces LIAS for students



Secure-connect.psu.edu



firewall_info



Firewall Team PRTG



PAN1



PAN2



PAN3



Splunk



Netscout Sightline



Remote Desktop
Applications



Remote desktop apps

←

→

↺

🏠

secure-connect.psu.edu/https/fbgprapp.fbit.psu.edu/RDWeb/webclient/index.html

☆

📄

🔍

⚙️

🔑

Ed

⋮

Apps

VTB: Global Protect...

FW Team Triage an...

VTB: FW Team - Enc...

VTB: FW Team - Pri...

Service Forms - Pen...

DCS Firewall Config...

Employee Depend...

Penn State IT Knowl...

Penn State Firewall...

Yammer : Home

Penn State Current...

»

All Resources

↗️

⚙️


⋮


👤


^


Privacy settings for managed resources have been preset by your organization. [Learn More](#)


GlobalProtect


PuTTY


Remote
Desktop...


TS Agent -
F1FAP-R...


TS Agent -
F1FAP-R...


VNC Viewer

RDP



← → ↻ 🏠 🔒 secure-connect.psu.edu/https/fbgprapp.fbit.psu.edu/RDWeb/webclient/index.html ☆ 📄 ⚙️ 🔑 Ed ⋮

Apps 🖨️ VTB: Global Protect... 🖨️ FW Team Triage an... 🖨️ VTB: FW Team - Enc... 🖨️ VTB: FW Team - Pri... 🖨️ Service Forms - Pen... 🖨️ DCS Firewall Config... 🖨️ Employee Depend... 🖨️ Penn State IT Knowl... 🖨️ Penn State Firewall... 🖨️ Yammer : Home 🖨️ Penn State Current...

⋮ All Resources 🖨️

Remote Desktop Connection

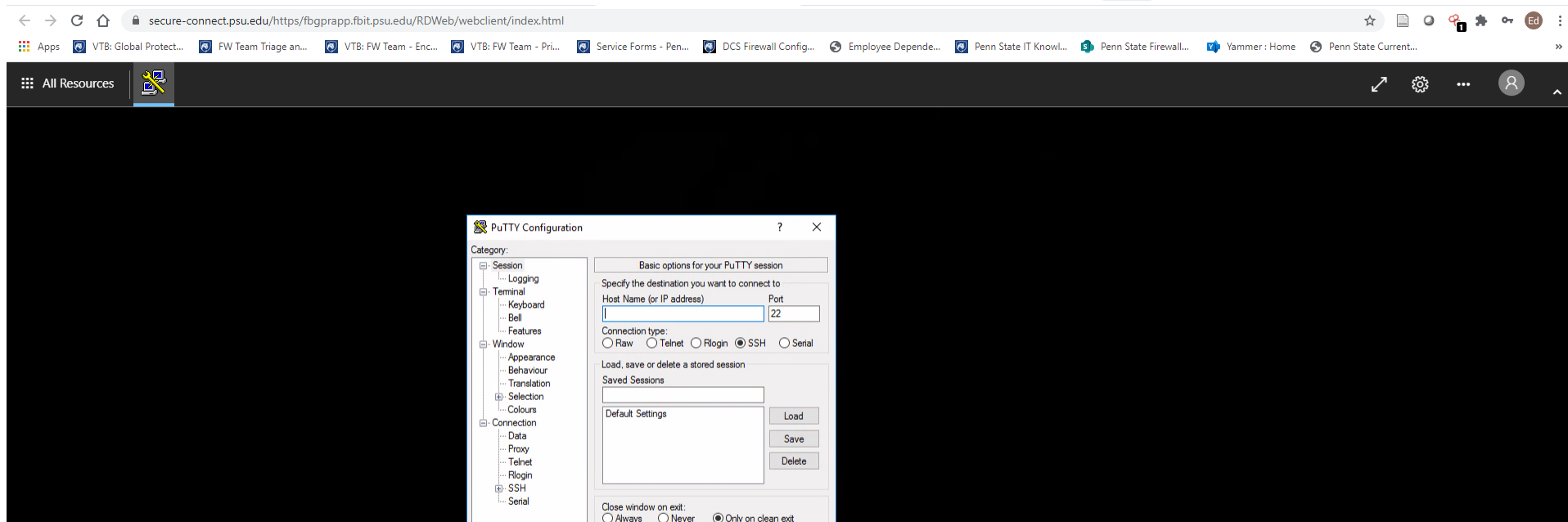
Remote Desktop Connection

Computer:

User name: None specified

The computer name field is blank. Enter a full remote computer name.

Show Options





Default posture per gateway

	Pre-Logon	Faculty/Staff (Managed and Unmanaged)	Student	Contractor
Internet	Default-Deny ¹	Managed on EFW	Managed on EFW	Default-Deny ²
Data Center	Default-Deny ¹	Managed on DCFW	Managed on DCFW	Default-Deny ^{1 2}
Unit LAN	Default-Deny	Default-Deny ²	Default-Deny ²	Default-Deny ²

¹ More specific permit rules have been implemented to provide needed functionality(DNS, AV updates, etc.)

² Unit-specific exceptions will be identified during onboarding engagement



Secure People

Secure Mobile Workforce

- Group Segmentation
- Role-based Access



Secure Resources



Units • Data Center • Enclaves



Secure Resources



Unit Resources

- Denied by default
- Application & Service based access by request
- User access is managed by you (unit admins)



Secure Resources



Data Center Resources

- User tunnels permitted by default
- Access managed on the Data Center Firewalls
- Access allowed according to the same userID information from GlobalProtect



Secure Resources



Enclaves

- Approved for secure enclave access
- Must pass an advanced device posture assessment
- Remote enclave secure endpoint access restricted by EAD security group



Initial onboarding challenges

- No standard OS images
- End users with poor internet
- Competing priorities for local IT staff
- Everyone is already remote



Working through challenges

- End user troubleshooting
- End user testing
- [Speedtest.psu.edu](https://speedtest.psu.edu)



PennState

Penn State Speedtest

Start

Ping

15.8_{ms}

Jitter

6.36_{ms}

Download

19.6

Mbps

Upload

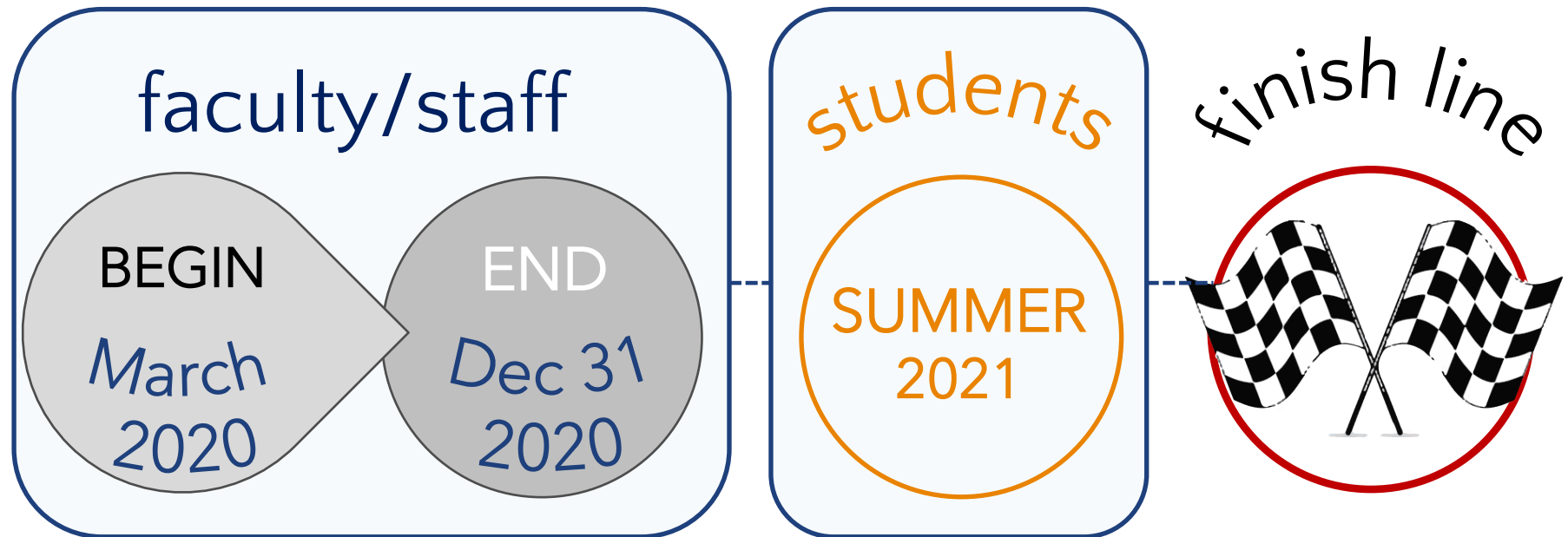
12.0

Mbps

10.40.147.189 - private IPv4 access



WHEN



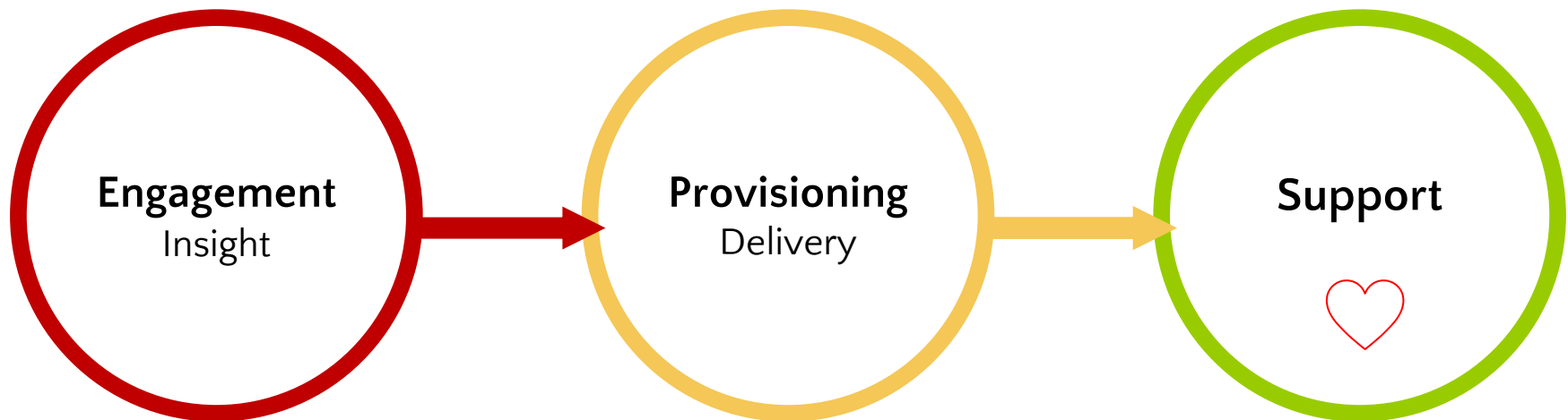


WHO

- Remote Access Needs
- On-premise
 - Enclave access
 - Other user-restricted access available



HOW





3 — How we can help you prepare —

Knowledge • Engagements • Communications Tools



Current Knowledge Base Articles

Public Facing

- [\(KB0013431\)](#) High-Level Transition
 - [\(KB0013419\)](#) Windows OS
 - [\(KB0013420\)](#) Mac OS
 - [\(KB0013424\)](#) Linux OS
 - [\(KB0013422\)](#) iOS Devices
 - [\(KB0013423\)](#) Android Devices

IT Facing

- [\(KB0013427\)](#) Technical Information
 - [\(KB0013524\)](#) IP Pool Allocations
 - [\(KB0013418\)](#) VPN Help
 - [\(KB0013671\)](#) Supported Agent Version
 - [\(KB0013417\)](#) Machine-based Certificates



4

How users get help with GlobalProtect

- Visit the IT Help Portal
- Call us at 814-865-HELP (4357)
- Email ITservicedesk@psu.edu
- Email us at firewall-team@psu.edu



Special Thanks

Don Welch/Rich Sparrow

OIS Support

Bill Wrobleski and Tim Shortall

Infra Leadership

EAD/IAM team

PKI support for Pre-Logon

Jody Harpster and Josh Miller

College of Education

Sysman Group

Client Packaging

Liberal Arts

Beta Customer and Early Adopter

Finance and Business IT

Backend Server Support and Early Adopter

Patty Rees and Greg Fox

Customer Experience

Firewall and Security Team



5 — Questions and answers



Thank you.