Considerations When Planning Your Deployment
Application Requirements

• Thin vs. Thick client considerations
• Connectivity requirements for applications
• How do your remote users work (network attached, offline data, cloud services, etc.)
BYOD vs Corporate Endpoints

• Potential support issues

• Implementing GP for both types of clients

• Detecting corporate endpoints
  – Device Certificates
  – Custom settings
  – Known processes
Cloud Services

• Be aware of data stored in cloud services
• Be aware of access controls for cloud services
• Protect your cloud data no matter where it is accessed from

Traditional VPN solutions fail because they were not built for this era of ubiquitous connectivity
User Experience

• Always-on vs. On-Demand agents

• Consider user experience changes from existing solutions

• Ensure there is good communication about changes

• Get backing from business unit leader
Case Study 1
Migration From Existing Network Layer VPN solution
Summary

Problem:
The client was running a traditional remote access solution that was nearing end of life.

The client wanted a solution that made it easier to protect their remote devices, internal networks, and alert on threats involving their remote users.

Solution:
Remote users were migrated to PAN GP to provide these features and allow management of remote access events through existing Panorama infrastructure.
Requirements

• Support both BYOD and Corporate Assets
  – Restrict access for BYOD devices to Citrix applications and RDP to VDI systems
  – Grant corporate assets “full” network access

• Perform HIP checks for corporate assets

• Split tunneling must be disabled for all clients
GlobalProtect Decision Points

• Simplify Operational Environment
  – Leverage existing hardware already deployed

• Improve Security Controls
  – Extend the same protection provided for local devices to remote devices (Wildfire, AppID, etc.)

• Improve Threat Visibility
  – Leverage existing threat detection processes for local and remote devices, through the same framework
Legacy Solution Overview
Legacy Solution Overview

Security policies for remote users exist in VPN appliance
Legacy Solution Overview

Security policies for remote users exist in VPN appliance

Limited security controls

Internet

Corporate LAN

Legacy VPN Appliance
Legacy Solution Overview

Security policies for remote users exist in VPN appliance
Limited security controls
Separate logging, monitoring, and management from other security devices
Legacy Solution Overview

Corporate Laptops and personal systems treated the same.
Legacy Solution Overview

Corporate Laptops and personal systems treated the same

Once VPN tunnel is established, both have full access to corporate network
GlobalProtect Solution Overview

Separate zone created for remote user connections
GlobalProtect Solution Overview

- Separate zone created for remote user connections
- Access to internal systems controlled by firewall security policies
GlobalProtect Solution Overview

Corporate assets establish VPN tunnel and are connected to Remote User Zone.
GlobalProtect Solution Overview

Corporate assets establish VPN tunnel and are connected to Remote User Zone.

Policies using HIP checks detect corporate assets and permit full connectivity.
GlobalProtect Solution Overview

BYOD assets establish VPN tunnel and are connected to Remote User Zone.
GlobalProtect Solution Overview

BYOD assets establish VPN tunnel and are connected to Remote User Zone

Policies using HIP checks detect non-corporate assets and restrict access
Lessons Learned

• Removal of legacy VPN client was problematic on some BYOD devices

• HIP Check illustrated problems with patching / AV updates on corporate assets

• Permit access to remediation services on your network to help resolve issues
Case Study 2
Migration From an Existing SSL VPN Solution
Summary

Problem:
The client was running an SSL VPN solution that performed application layer tunneling for specific applications.

Corporate assets were getting infected with ransomware when outside of the protection of the corporate network.

More than once, malware was not discovered until systems reconnected to the corporate network.

Solution:
All remote users were migrated to GlobalProtect to provide improved security controls over remote access and remote devices.
Requirements

- Support both BYOD and Corporate Assets
  - Restrict access for BYOD devices to Citrix applications and RDP to VDI systems
  - Grant corporate assets “full” network access
- Perform HIP checks for corporate assets
- Split tunneling must be disabled for all clients
GlobalProtect Decision Points

- Customer wanted better security controls
  - Advanced threat protection (Wildfire, AppID)
  - Policy rules based on UserID, not just IP address
- Replaced remote access, web filtering, IPS
  - Reduced environment complexity by replacing multiple security platforms with PAN NGFWs
Legacy Solution Overview

Security policies for remote users exist in VPN appliance.
Legacy Solution Overview

Individual apps are proxied via SSL to the SSL VPN appliance.
Legacy Solution Overview

Proxied app traffic permitted to internal hosts
Legacy Solution Overview

App layer control does not disable split tunneling

Remote systems have full Internet connectivity while running apps via SSL VPN
GlobalProtect Solution Overview

Corporate & BYOD assets establish VPN tunnels to Remote User Zone

Policies using HIP checks enforce rules by host type
Lessons Learned

• SSL VPN users not pleased with changes from the legacy solution:
  – No more split tunneling
  – No splash screen with links to click on to launch apps
  – GP client visibly running in their system tray
More Lessons Learned

• Get a champion for the new solution from each of your business units

• Communicate user experience changes ahead of time

• GlobalProtect client much easier to support than browser plug-in / java applet based solutions