APRIL 3-6, 2016 | LAS VEGAS | THE COSMOPOLITAN
Practical Advice for Planning Security Segmentation
Things to think about...

• Perform segmentation where there is going to be a benefit
  – Higher risk areas where you need more visibility or control
  – Areas where you can quantify required applications, clients, and servers
Things to think about...

• Identify common services that you will need to enable, in addition to client-server application traffic:
  – Administrative access (SSH, RDP, SNMP, etc.)
  – Network Service access (DNS, NTP, Active Directory, etc.)
  – Management System Access (PIM, NMS, Backups, AV, Patch Management)
Things to think about...

- Watch out for too much complexity in policies
- Test thoroughly before implementing policies
  - Some applications may require discovery
  - Use ‘permit any/any log’ rules to identify requirements
  - Set firm deadlines for discovery rules to be removed
  - Don’t be surprised if you break some applications
Things to think about...

• Monitor performance as you add zones / rules
  – Disable logging for chatty services (i.e. DNS)
  – Consider modifying network architecture to route some traffic around security devices
  – Consider the modular chassis so performance can be added as your security segmentation increases
Case Study 1

Critical Application Access From the Corporate Network
Summary

Problem:
The client’s corporate network did not meet security requirements for protecting its critical applications.

Solution:
Critical applications were placed in separate security zones, protected by PAN NGFWs.

GlobalProtect was implemented to ensure that only authorized users, on authorized devices, were granted access to these applications.
Requirements

• Enforce token-based multi-factor authentication for system access
• Ensure only specific corporate managed devices are permitted to connect
• Perform basic HIPS check on clients (AV status check)
• Block access to other networks (internal and external) by clients while connected
Requirements

• Support proprietary thick client applications
• Provide detailed authentication and access logging to SIEM systems
• Permit access to different protected systems based on AD group membership
GlobalProtect Decision Points

• Internal segmentation without complex policies
  – AppID / UserID policies in place of IP / Service policies
  – Ability to enable IPS on individual rules, not just globally

• Ability to grant access to critical systems based on clients security posture
Network Architecture (Before)
Network Architecture (w/ Segmentation)
Network Architecture (w/ Segmentation)

Corporate Network

Critical Application Zone

Internet

Application Servers

Database Servers

Admin Workstations
Network Architecture (w/ Segmentation)

Internet

Corporate Network

Authorized Clients

Application Servers

Database Servers

Admin Workstations

Critical Application Zone
Network Architecture (w/ Segmentation)

While connected to critical apps through GP gateway, no other Networks are accessible
Lessons Learned

• Communicate Changes Early and Often
  – Drastic changes to user experience (previously directly connecting to apps/servers)
  – Drastic changes to IT Ops / Access Management philosophy
  – Buy-in from leadership

• “Deny any except required” vs. “Allow all except known bad”
Lessons Learned

• HIP checks shine light on other issues
  – Patch management problems
  – Antivirus updates may be unreliable

• Certificate management is not always fun
Case Study 2
Secure Access For MSP
Support of Branch Devices
Problem:
The client had a large network with offices distributed across a large geographic area.

An MSP was used to service equipment connected to the network at these branch sites.

Solution:
Field techs used GP with cellular, or wired connections at branch sites, to access services on the network to perform maintenance and troubleshooting tasks.
Requirements

• Allow limited access to require resources for third party technicians
• Support mobile (cellular) device connectivity for NMS applications
• Support secure wired connectivity for specific applications
• Support custom field applications
Requirements

• Types of applications / access
  – NMS (accessed by cellular and wired clients)
  – Proprietary apps (wired)
  – File repository (wired)
  – Trouble shooting tools (ICMP, SSH, HTTP)
GlobalProtect Decision Points

• Support for mobile and traditional devices
  – Ability to apply policies based on mobile device details (IMEI, phone number, jailbroken, etc.)
  – Common platform for supporting / monitoring all types of devices

• Leverage existing hardware to improve control / monitoring of MSP activity
Network Architecture

Data Center LAN

Internet

Branch WAN

3rd Party Managed Equipment

Corp Equipment

Network Components
Network Architecture

Field equipment Managed by 3rd party MSP
Network Architecture

NMS and CCM servers managed by internal staff

Servers are used to support other corporate systems

Field equipment Managed by 3rd party MSP

- Data Center LAN
- Branch WAN
- Internet

3rd Party Managed Equipment

Corp Equipment
Network Architecture

After replacing equipment, field techs log in via mobile device to check device status in NMS.
Field techs can access configuration management server via wired connection to perform deeper troubleshooting.
Lessons Learned

- Management of mobile devices can be tedious; leverage MDM to help manage devices

- MSP users tend to report everything as “a firewall issue”

- Performance issues sometimes difficult to nail down (client, network, server)