Telework Reference Architecture

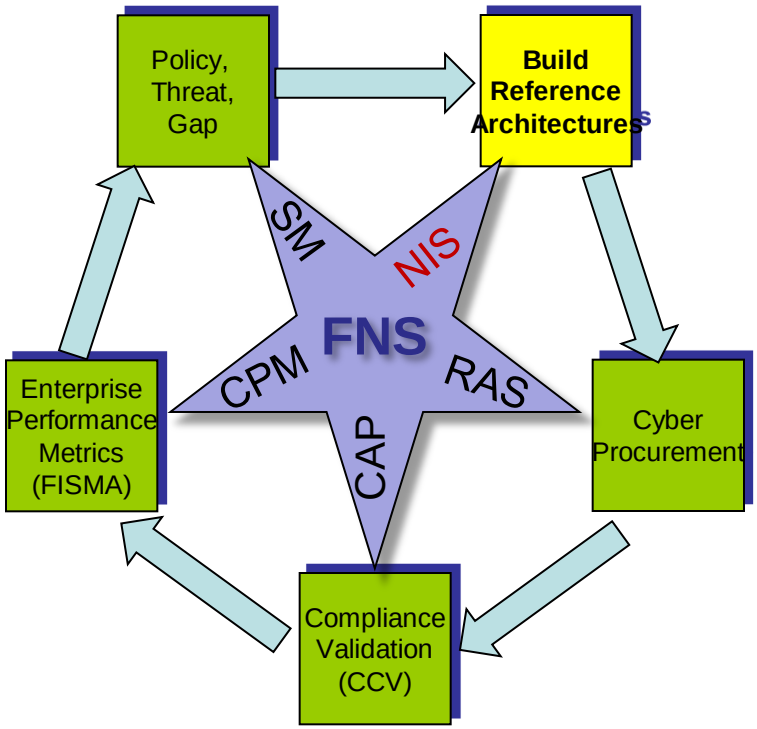
October 13, 2011

FEDERAL COMPUTER SECURITY PROGRAM MANAGERS' FORUM

Oscar Ahumada
Telework R/A Project Manager
Oscar.ahumada@DHS.GOV

So Who Am I?

- Federal Network Security
  - Identify new cyber policy, threat, or opportunity
  - Policy prompts design of new architecture
  - Architecture drives cyber procurements
  - DHS validates agency compliance
  - Agencies submit enterprise performance metrics
- Physically and Organizationally co-located with U.S. CERT

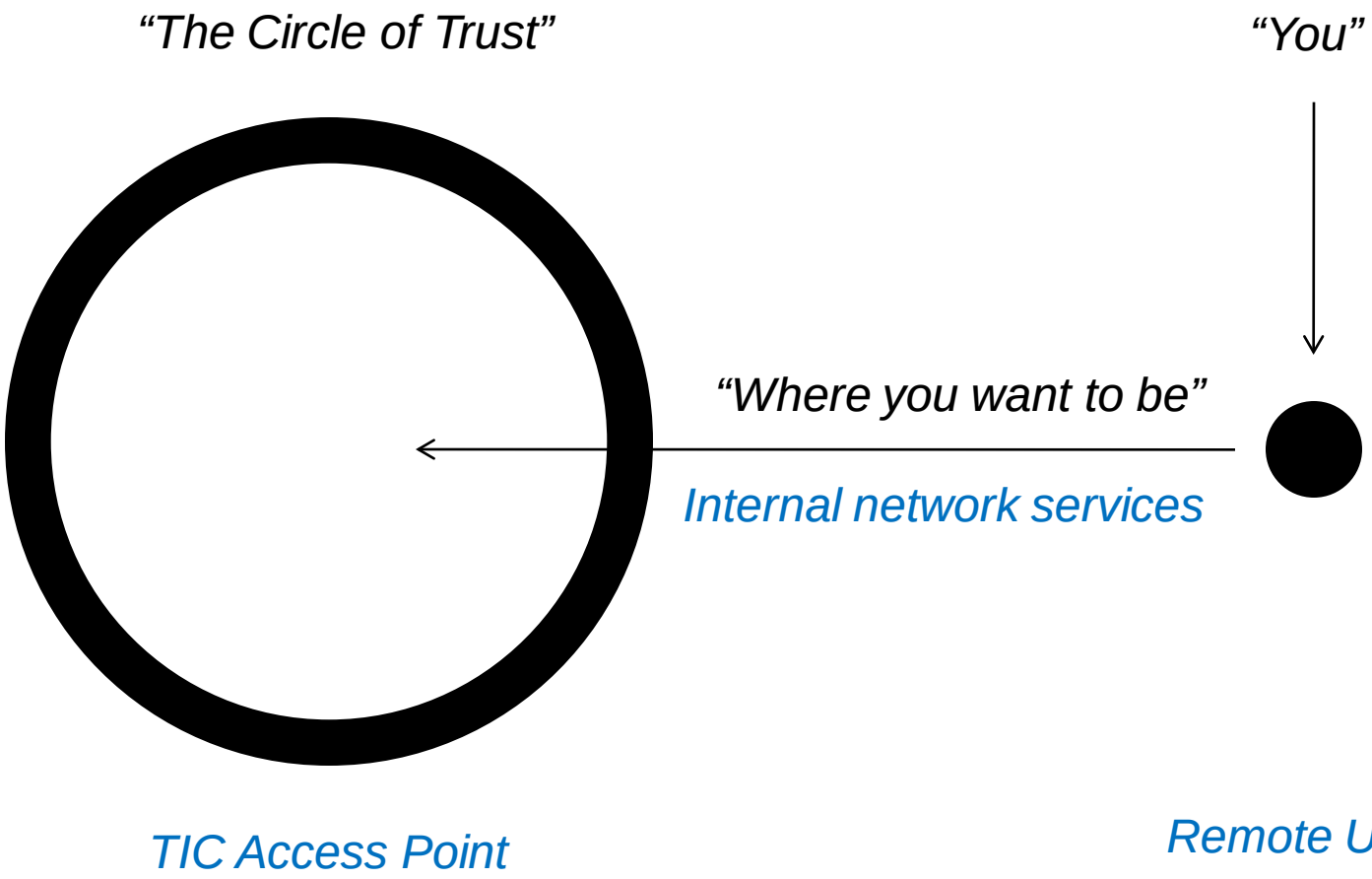


Goals the Telework Reference Architecture

- Purpose:
  - Provide technical guidance to agencies implementing the Telework Enhancement Act of 2010, OMB M-11-20, and OMB M-11-27
  - Strengthen D/A mobility effectiveness
  - Improve Continuity of Operations (COOP)
  - Enhance Work-life Balance

- Goals:
  - Document best practices implemented by volunteer model agencies
  - Identify what D/As need for a secure and functional Telework system
  - Identify key issues preventing D/As from complying to current security mandates
  - Feed results into the FISMA, CCV, and procurement processes
  - Guide D/As to meet mandated requirements

What do you technically mean by “Telework”?



Telework R/A Current Status

- Version 1.3 released 11 Oct 2011
  - All versions are available on our OMB MAX website
  - Work Group meetings conducted 26 August and 30 September
  - Agency Interviews conducted
    - ATF: 1 Sep
    - DOI: 8 Sep
    - NIST: 19 Sep
  - Agencies have provided numerous recommendations and feedback for improvement
  - Final version due 17 October

R/A Sections

- Background:
  - Summary of legal and policy guidance
- Scope:
  - Unclassified systems
  - Untrusted networks
  - GFE Focus (but also discusses non-GFE)
  - Out of Scope: mobile systems
- Technical Constraints:
  - TIC 2.0 compliant access point
  - USGCB compliant workstation

Telework Threats

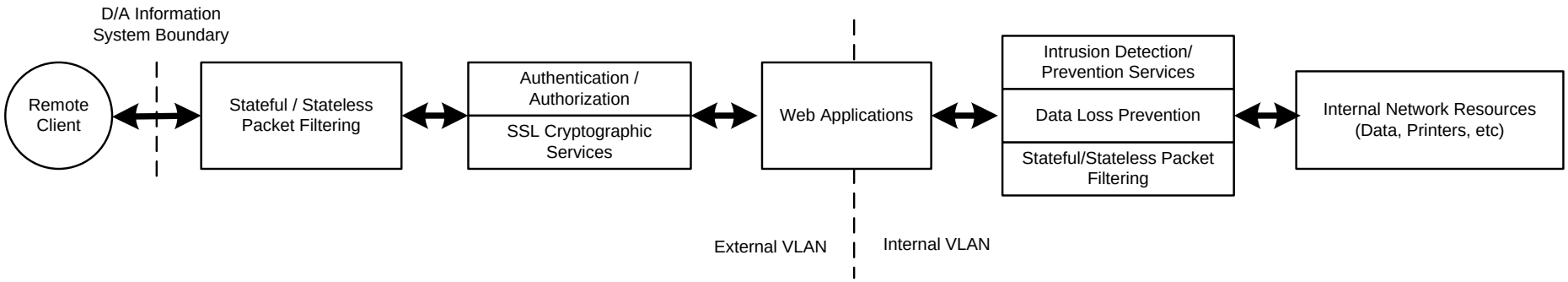
Threat Category	Description
Denial of Service	Attacker prevents or prohibits the normal use or management of networks or network devices.
Man-in-the-Middle	Attacker actively intercepts the path of communications between two legitimate parties, thereby obtaining authentication credentials and data. Attacker can then masquerade as a legitimate party.
Masquerading	Attacker impersonates an authorized user and gains certain unauthorized privileges.
Message Replay	Attacker passively monitors transmissions and retransmits messages, acting as if the attacker were a legitimate user.
Traffic Analysis	Attacker passively monitors transmissions to identify communication patterns and participants.
Malware and Malicious Users	Attacker is either an infected authorized remote client, or a potential insider threat.
Residual Information	All telework architectures have the potential to leave some trace of their operation on the remote client device. This residual information can range from cryptographic keys to entire files cached on disk.

Telework Architectures

- Web Application
- Virtual Desktop
- Host-to-Gateway
- Host-to-Gateway + Virtual Desktop

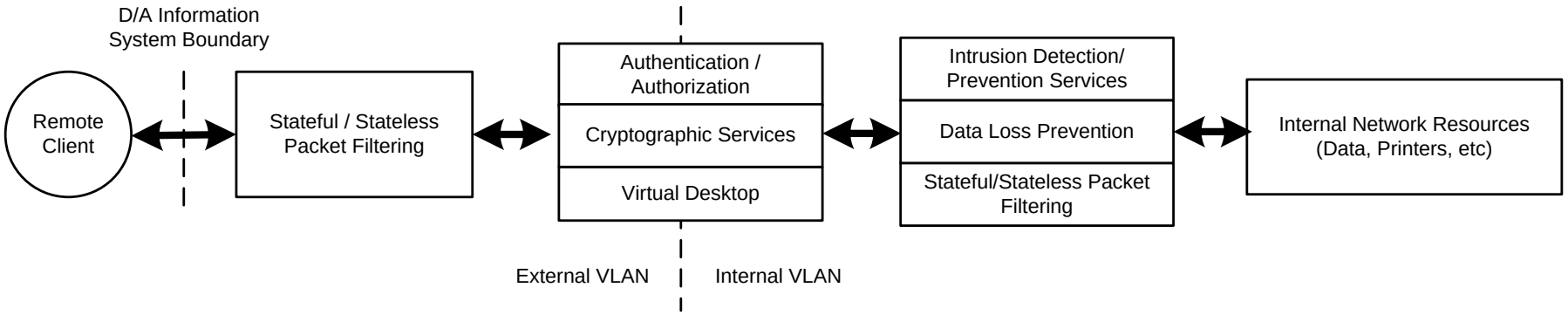
Web Application

- Benefits
  - Minimal external network footprint
  - Minimal remote client setup
  - Based on widely adopted and supported standards
  - Continually growing range of applications available
- Drawbacks
  - Internal data sent to remote client
  - Limited use of other network protocols
  - Limited application availability



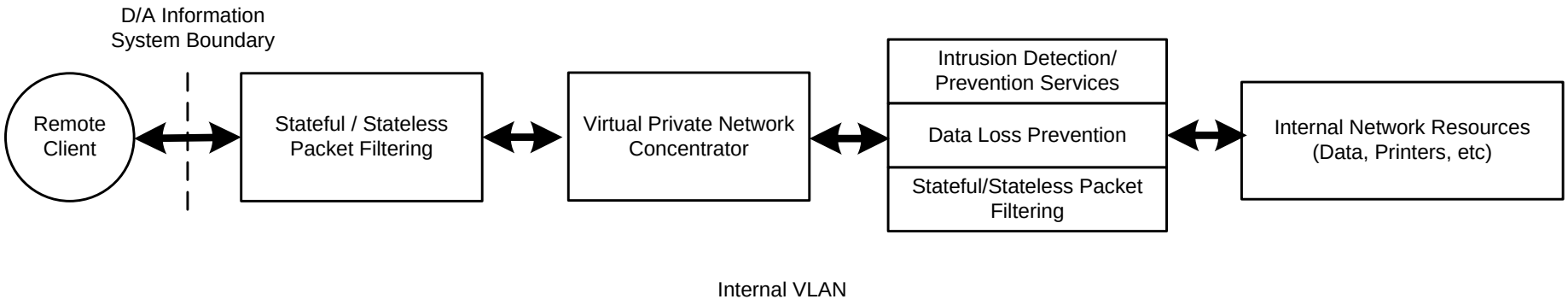
Virtual Desktop

- Benefits
  - Highly functional environment, similar to a local desktop experience
  - Data remains within the D/A information system boundary
  - Central IT management of resources and policies
  - Simplifies policy enforcement
- Drawbacks
  - More IT support required to maintain the infrastructure
  - More costly infrastructure
  - Possible non-compliance with FIPS 140-2 cryptographic requirements
  - Bandwidth intensive



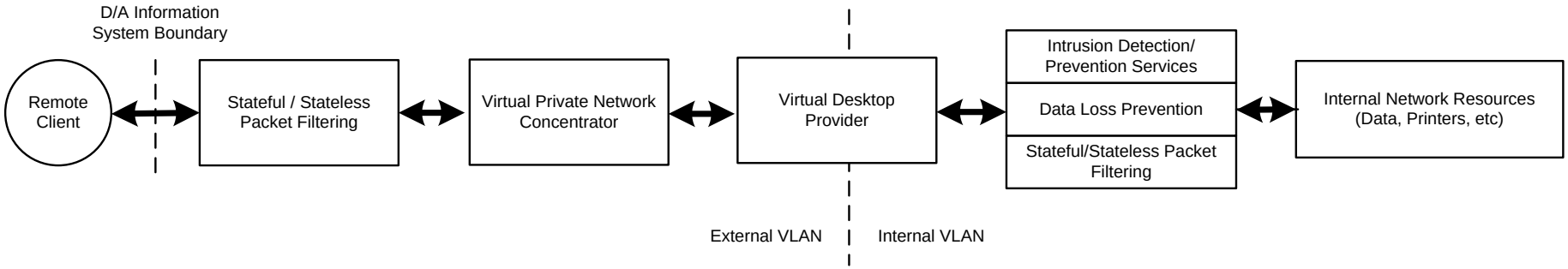
Host-to-Gateway

- Benefits
  - Local network access provides greatest access to network resources
  - Large number of network applications / protocols supported
  - Minimizes external network footprint
- Drawbacks
  - Exposure of internal network resources to potentially infected remote clients
  - Data utilized during sessions transferred to remote client
  - Limited ability to monitor / log activities
  - Trusted Insiders present the greatest threat



Host-to-Gateway with Virtual Desktop

- Benefits
  - Provides separation from internal network by using VDI as an intermediary
  - Centralized IT support of applications / desktops
  - Wide range of applications available to support the environment
  - Minimal exposed network footprint
  - Supports a wide array of clients and cryptographic protections
- Drawbacks
  - Greatly increased IT support required for virtual desktops
  - Potential for requiring multiple authentication databases that must be synchronized.
  - High bandwidth utilization per client
  - Potentially low throughput for VPN concentrator



Non-GFE Considerations

- 2 Methods
  - Disallow non-GFE devices
  - Tiered architecture allowing non-GFE to access certain resources

- Non-GFE Risks:
  - Misconfiguration
  - Malware
  - Information Control
  - IT Support

Security Functions

- Management
- Training
- Physical Controls
- Authentication
- Data Storage
- Configuration
- Secure Communications
- Traffic Inspection
- Packet Filtering
- Content Filtering
- Logging
- Monitoring and Auditing
- Response
- Reporting

Contact Information

- OMB Max Portal: https://max.omb.gov/community/display/DHS/Mobile+and+Telework+Access

- Project Lead: Oscar Ahumada
  Oscar.Ahumada@dhs.gov
- Technical Lead: Alex Nicoll
  anicoll@cert.org
- Project Support: Eric Pratsch
  Eric_Pratsch@sra.com

Questions