



**Process Control Systems
Industry Conference**

**Secure Access into
Industrial Automation and Control Systems**
Industry Best Practice and Trends

**Serhii Konovalov
Venkat Pothamsetty
Cisco**

Vendor offers a remote firmware update and PLC programming....

Contractor asks for access to SCADA from pipeline pump station...

Available industrial security guidelines do not detail Secure Access...

Agenda

- ◆ **Risks and Benefits**
- ◆ **Secure Remote Access into an IACS**
- ◆ **Secure Local Access into an IACS**
- ◆ **Secure Direct Access enabled by NAC**
- ◆ **Summary**

Remote and Local Access Parties

- ◆ Authorized employees, contractors, vendors
- ◆ External Security Center
- ◆ Standalone Remote Embedded Device
- ◆ Remote Control Center

And others....

Do not forget

- ◆ *Portable Storage Media*

Cyber Security Risks

- ◆ **Unauthorized/Unknown Access**
- ◆ **Inability to Limited Access**
- ◆ **Malicious and Mobile Code**
- ◆ **Accidental Misconfiguration**
- ◆ **Disgruntled Insiders**

...



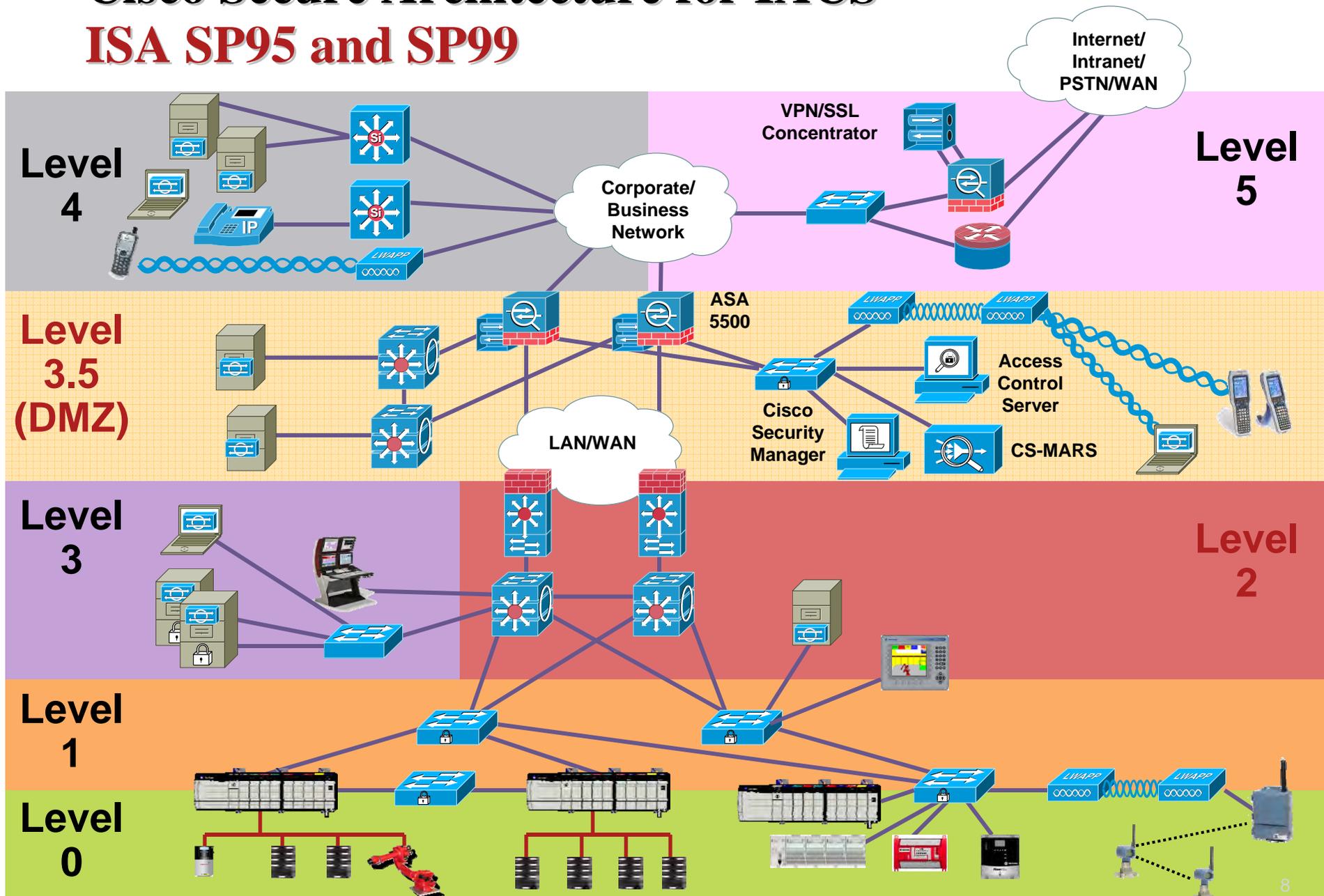
Business Risks

- ◆ **Loss of Revenue**
- ◆ **Unanticipated Costs**
- ◆ **Fines Due to Violation of Legal and Regulatory Requirements**
- ◆ **Safety Incident**
- ◆ **Adverse Press Coverage**



Cisco Secure Architecture for IACS

ISA SP95 and SP99



Business Benefits

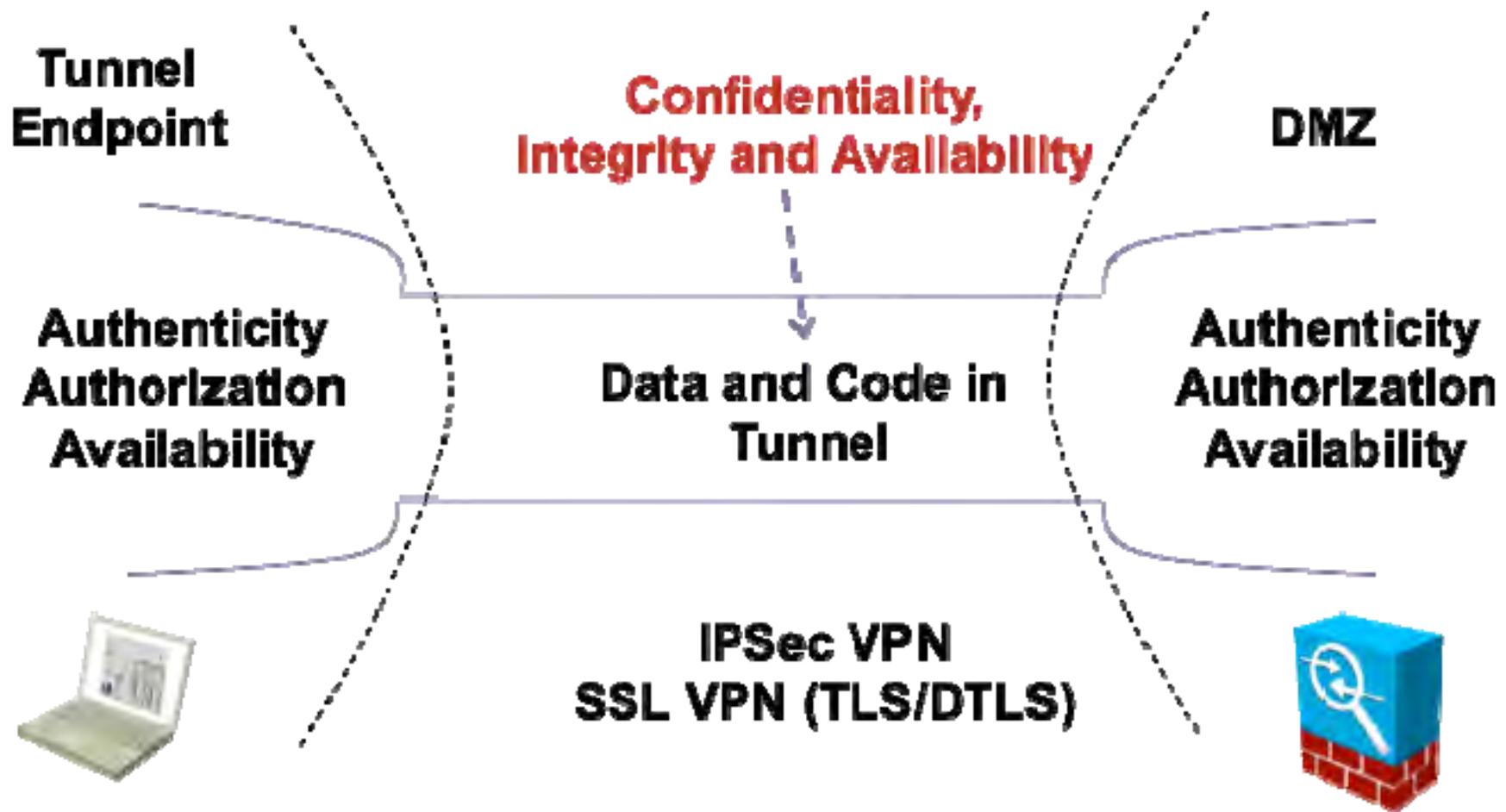
- ◆ **Reduce Total Cost of Ownership**
- ◆ **Improve Operational Efficiency**
 - Low-cost External Manufacturing and Engineering Support
 - Mobile Workers
 - Reduce Errors of Manual Input
- ◆ **Regulatory Compliance: Logging, Audit and Reporting of Access Attempts**



Agenda

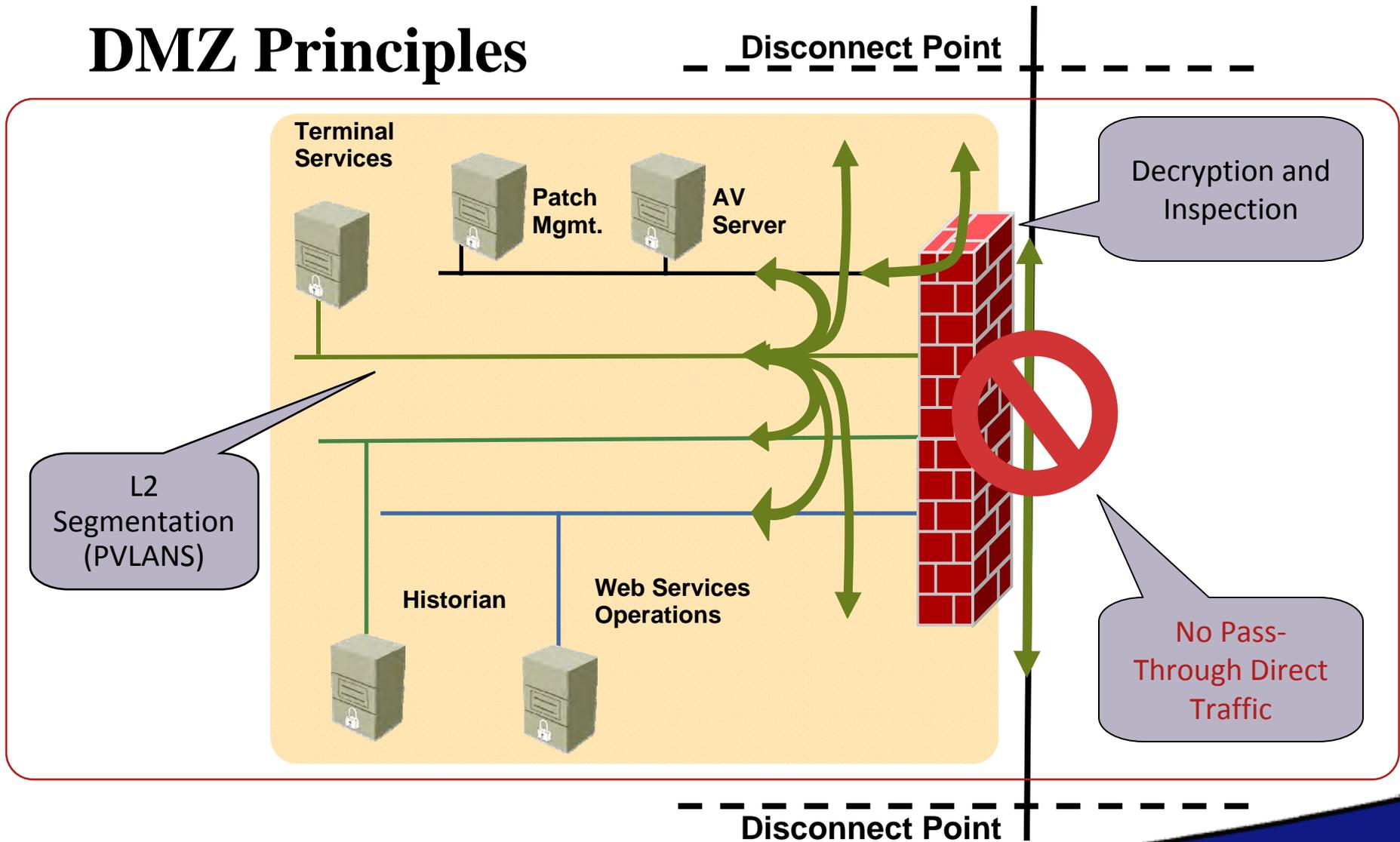
- ◆ Risks and Benefits
- ◆ Secure Remote Access into an IACS
- ◆ Secure Local Access into an IACS
- ◆ Secure Direct Access enabled by NAC
- ◆ Summary

Remote Access (RA) Security Requirements



* According to ISO/IEC 18029-5:2006

DMZ Principles



Other DMZ considerations of RA

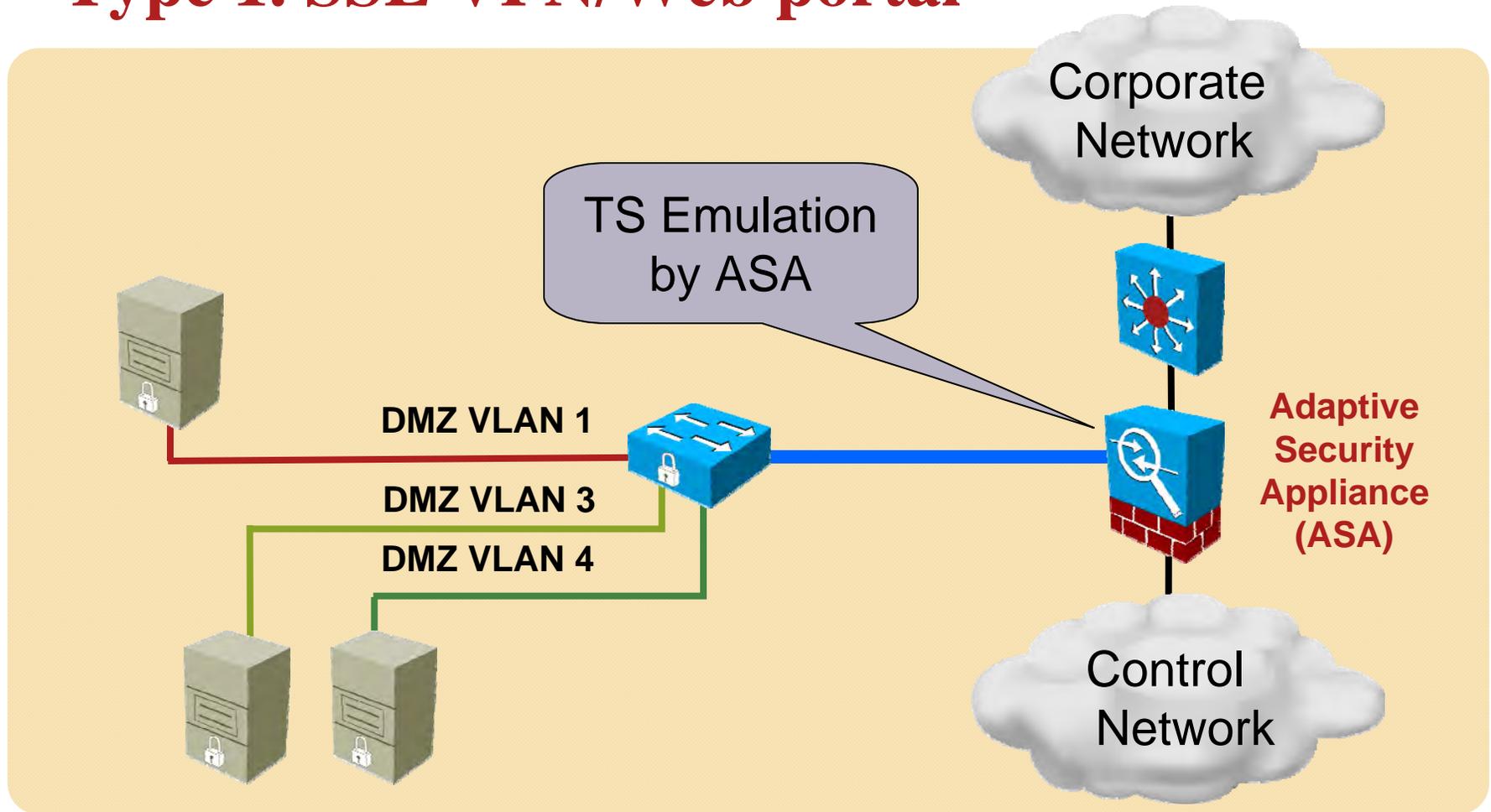
- ◆ “Client Less” VPN
- ◆ Role-Based Access Control
- ◆ **Bandwidth Adjustment**
- ◆ Intrusion Protection
- ◆ **Split-tunneling should be avoided**
- ◆ RDP Session Recording (metadata analytics)

Options of Secure Remote Access

- ◆ **Type 1: SSL VPN and WEB Portal**
- ◆ **Type 2: Service-Oriented RA**
- ◆ **Type 3: “Corporate IT” best-practice RA**

DMZ – Architecture for unmanaged devices

Type 1. SSL VPN/Web portal



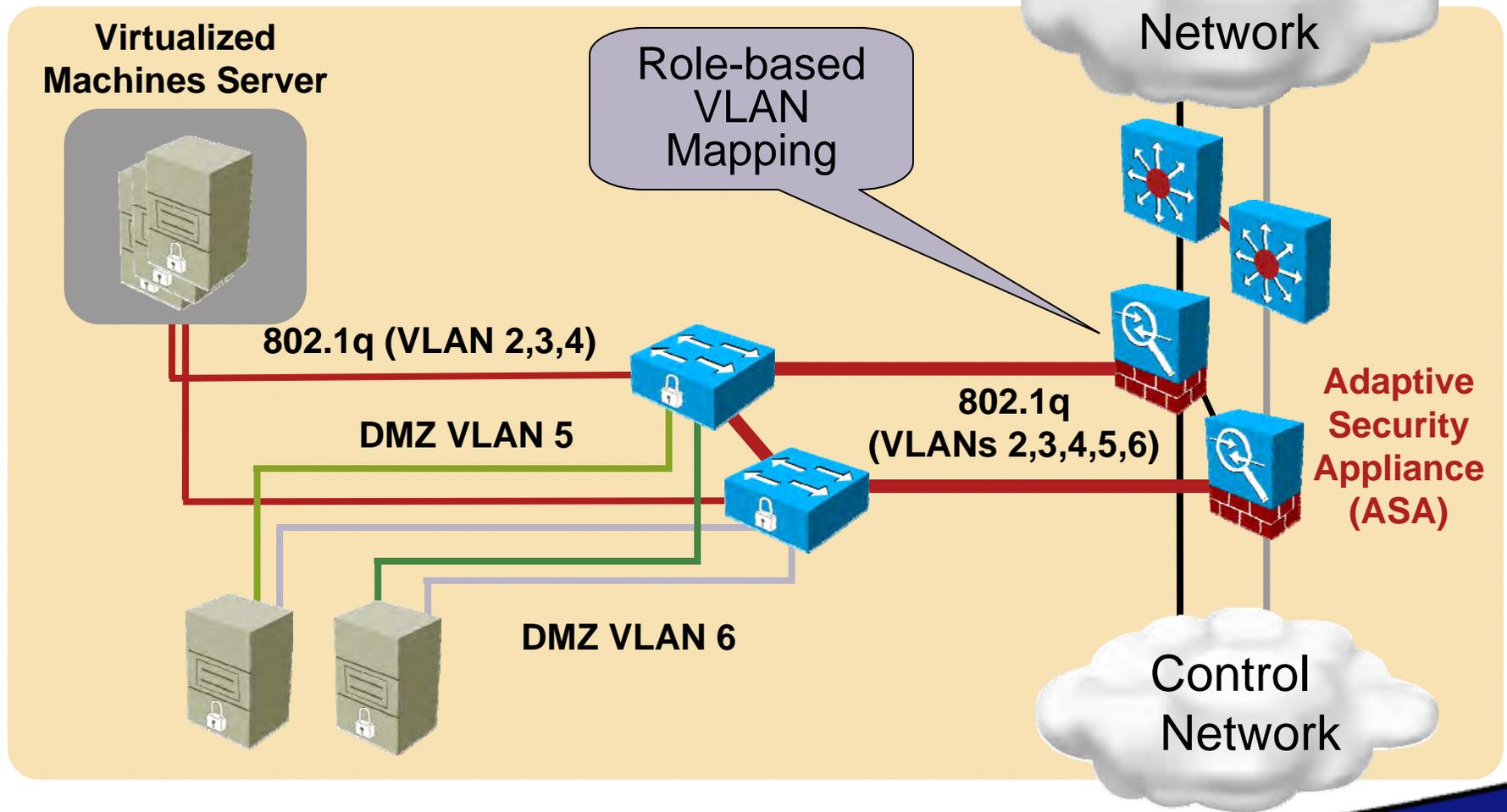
DMZ – Architecture for unmanaged devices

Type 1. SSL VPN/Web portal

- ◆ **No need for a Terminal Server**
- ◆ **Only SSL VPN mode**
- ◆ **Control Protocols doesn't pass through a DMZ firewall**
- ◆ **Available Single SignOn**
- ◆ **Terminal Session is not captured**

DMZ - Extended control for unmanaged access

Type 2. Service-Oriented RA



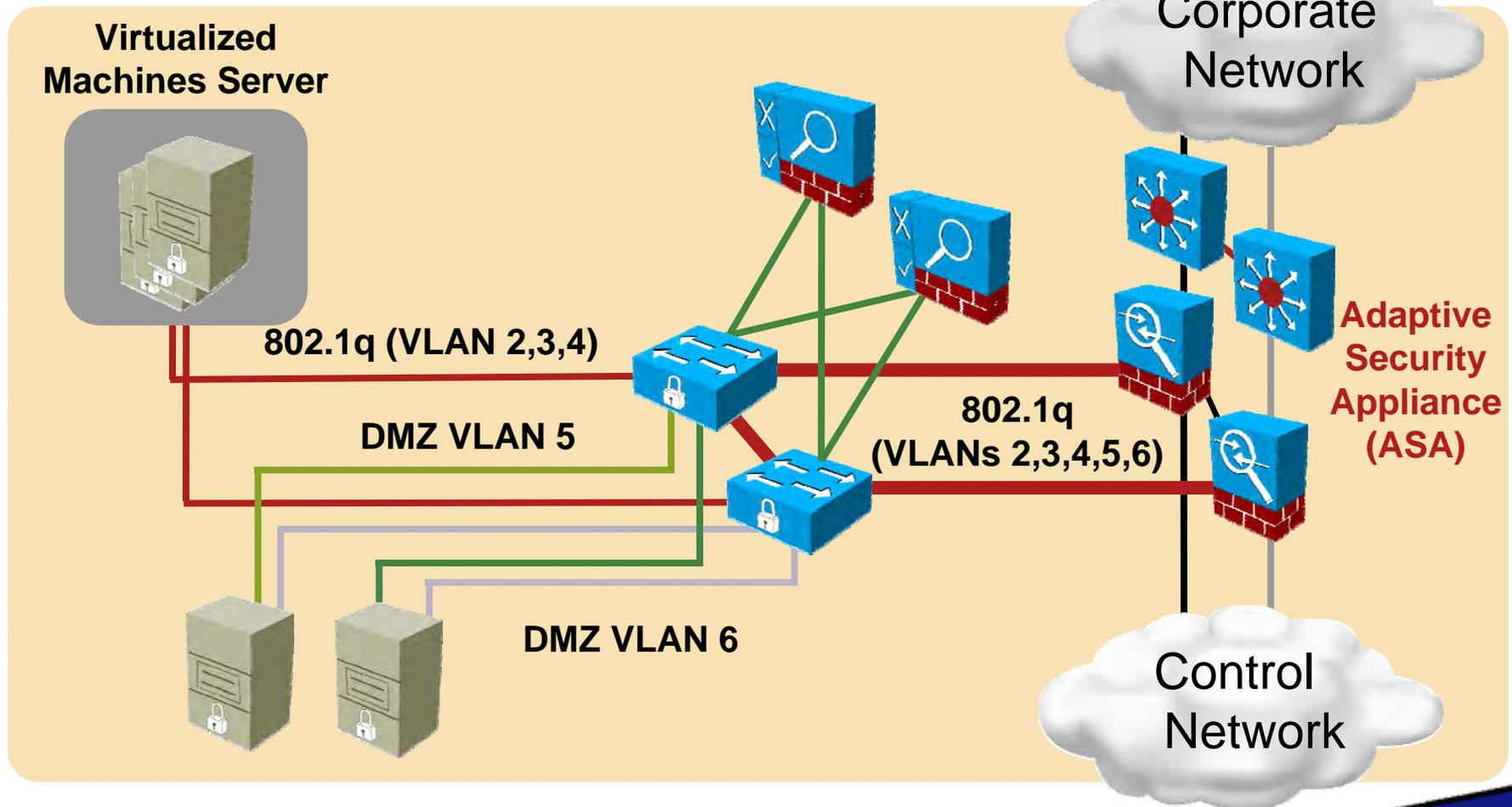
DMZ - Extended control for unmanaged access

Type 2. Service-Oriented RA

- ◆ IPsec and SSL VPNs
- ◆ All types of Authentication
- ◆ Granular Role-based Access Model
- ◆ Session Recording
- ◆ Single SignOn available (for TS Access)

DMZ – Enhanced Architecture

Type 3. “Corporate IT” RA



DMZ – Enhanced Architecture

Type 3. “Corporate IT” RA

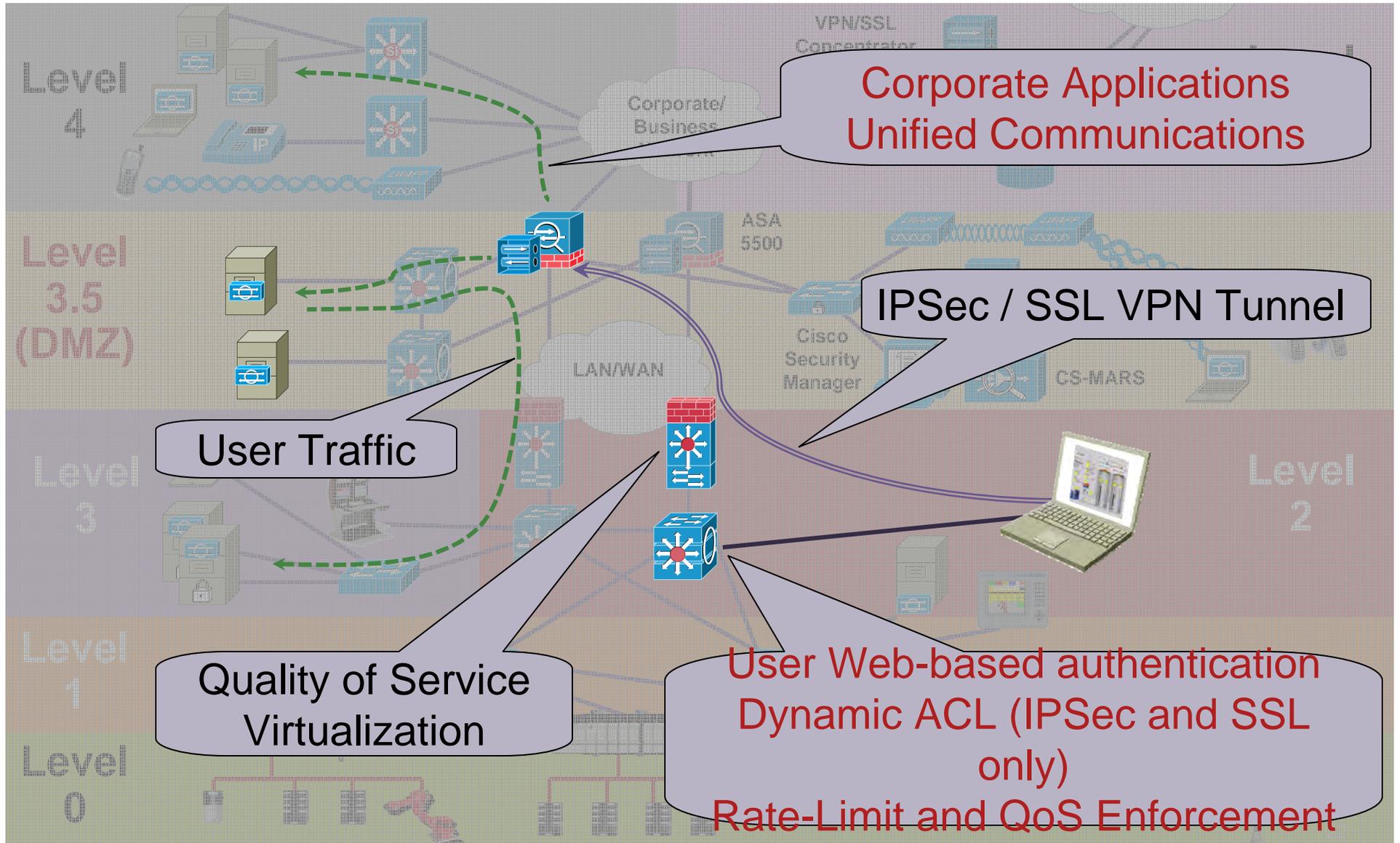
- ◆ **Enhanced and adjusted version of “Type 2”**
- ◆ **Corporate IT VPN Security Best Practice**
- ◆ **Security Policy Enforcement**
- ◆ **Quarantine and Remediate**
- ◆ **Managed and Unmanaged Endpoints**

Agenda

- ◆ Risks and Benefits
- ◆ Secure Remote Access into an IACS
- ◆ Secure Local Access into an IACS
- ◆ Secure Direct Access enabled by NAC
- ◆ Summary

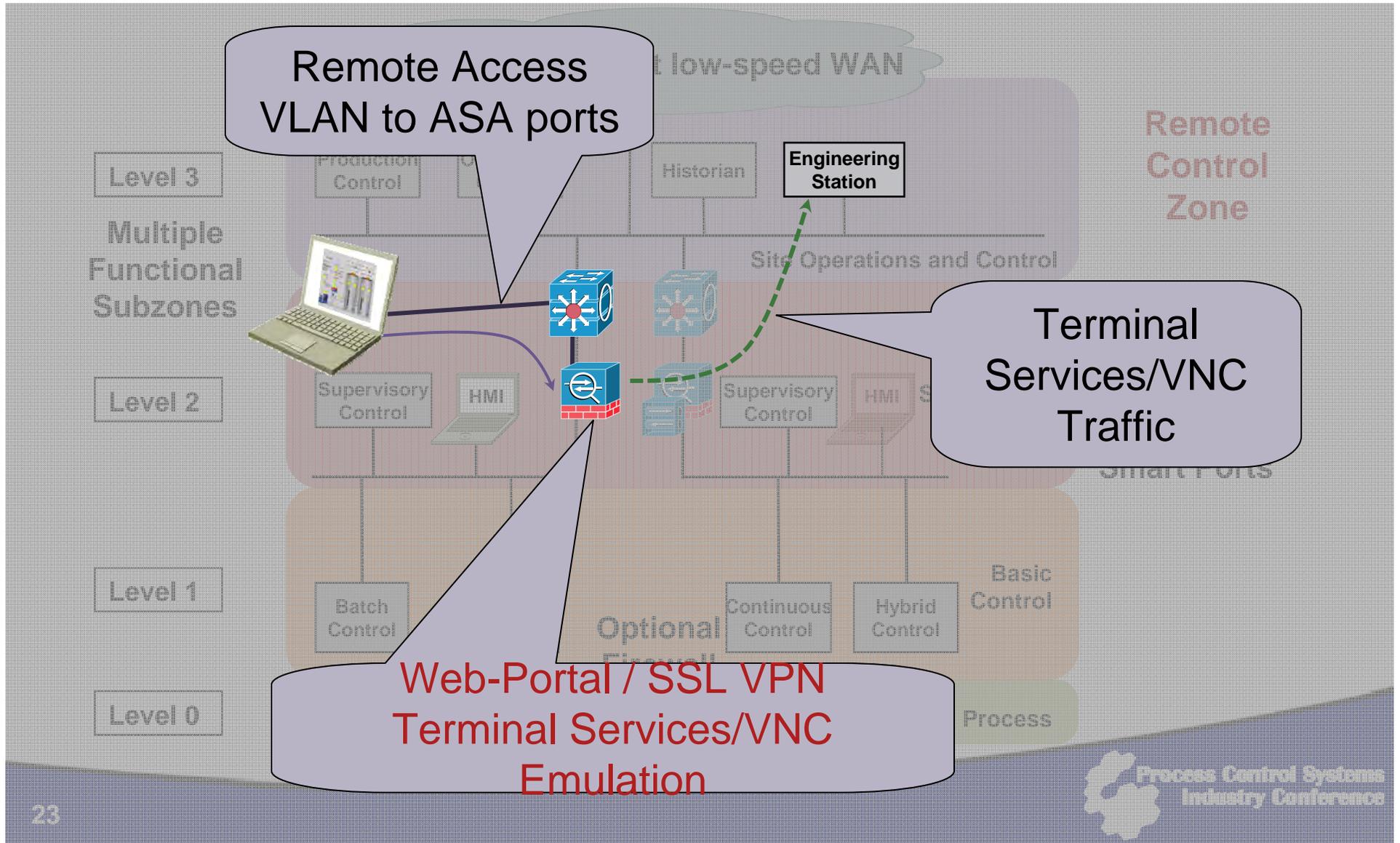
Secure Local Access into an IACS

Type 1. VPN-Based Local Access



Secure Local Access into an IACS

Type 2. Web-Portal Based Local Access

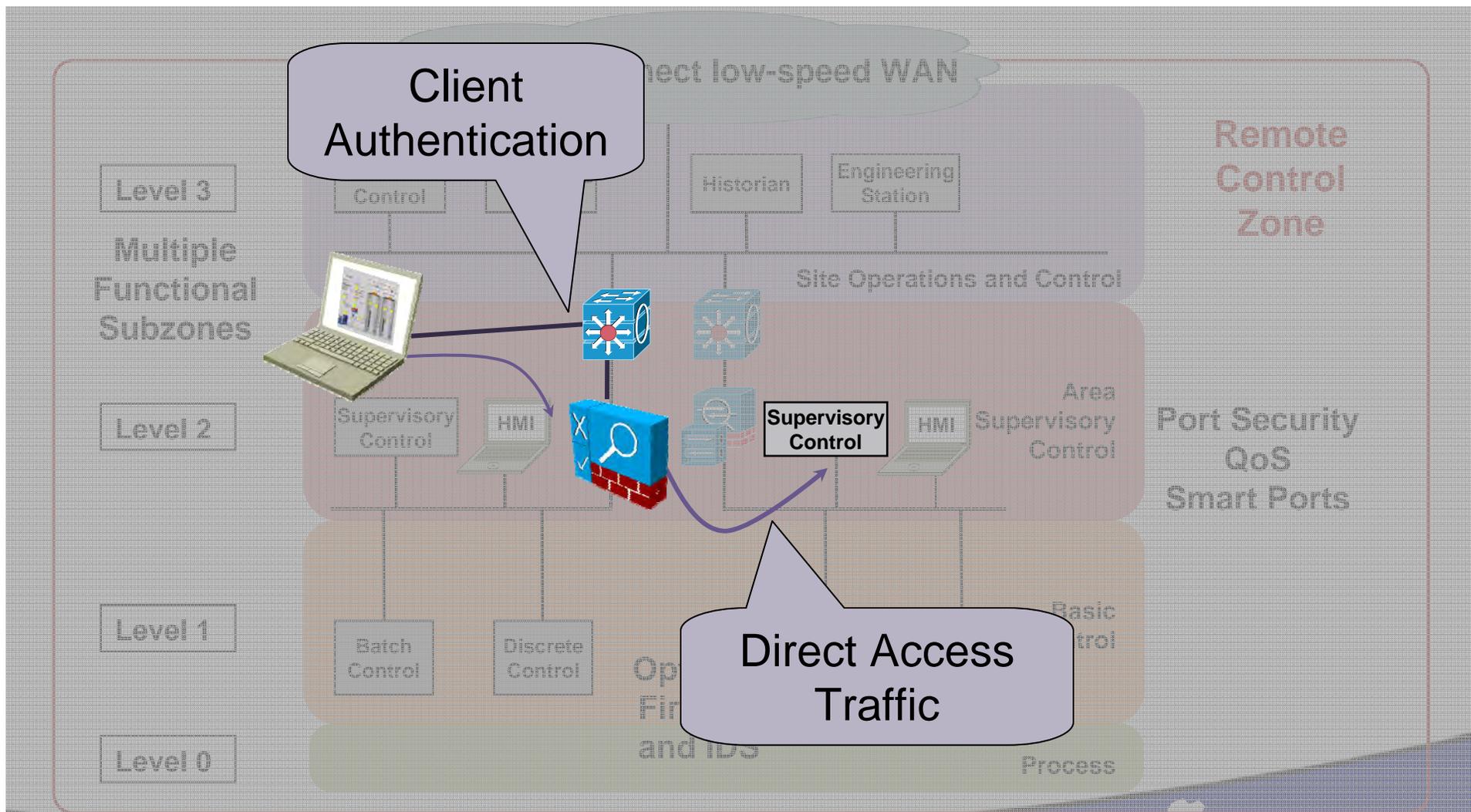


Agenda

- ◆ Risks and Benefits
- ◆ Secure Remote Access into an IACS
- ◆ Secure Local Access into an IACS
- ◆ Secure Direct Access enabled by NAC
- ◆ Summary

Secure Direct Access into an IACS

Network Admission Control



Network Admission Control (NAC)

- ◆ **Authenticates clients (users and devices) before allowing network (wired/wireless) access**
- ◆ **Checks client devices for security policy compliance**
 - Running HIPS (e.g. CSA), AV, patch current ...?
 - Clients that fail posture assessment placed on remediation VLAN
- ◆ **Helps prevent infection of ICS by mobile devices**
- ◆ **NAC Profiler identifies devices and enforces roles**
 - PLC? Vendor laptop? Employee? Network admin?
 - Role-based VLAN assignment
- ◆ **Appropriate for both DMZ (Remote access) and Control Zone (local access)**

NAC Components

◆ The Appliance

- Deployed out-of-band in CZ for device and user role enforcement
- Deployed in-band in DMZ to enforce remote access user roles
- NAC Profiler Collector runs on NAC Appliance

◆ The Profiler Server

- Resides in DMZ, works with multiple NAC Appliances

◆ The Manager

- Resides in DMZ, controls multiple NAC Appliances
- Device & user profiles specified on NAC Manager

NAC Profiler: Automated Profiling of Devices



PCs	Non-PCs		
	CZ Devices	Printer	AP
 	 PLC	 	

Discovery	<p style="text-align: center;">Endpoint Profiling</p> <p>Discover all network endpoints by type and location</p> <p>Maintain real time and historical contextual data for all endpoints</p>
Monitoring	<p style="text-align: center;">Behavior Monitoring</p> <p>Monitor the state of the network endpoints</p> <p>Detect events such as MAC spoofing, port swapping, etc.</p>

Automated process populates devices into the NAC Manager; and subsequently, into appropriate NAC policy

NAC Profiler Components



NAC Profiler Server

Aggregates all data from Collectors and manages database of endpoint information. Updates the Cisco NAC Appliance Manager, where roles are applied.



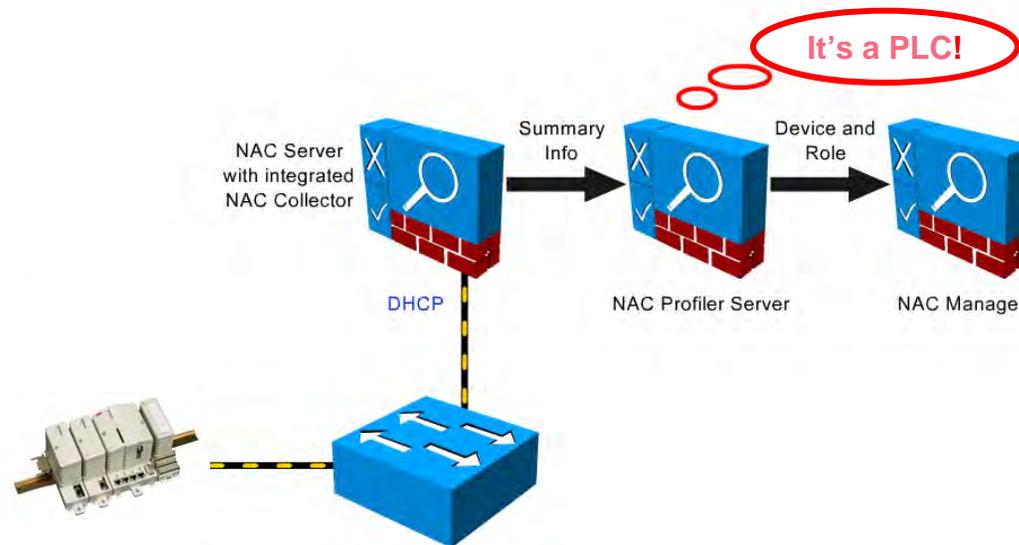
NAC Collector

Gathers information about endpoints using SNMP, Netflow, DHCP, and active profiling

Co-resident with NAC Appliance Server

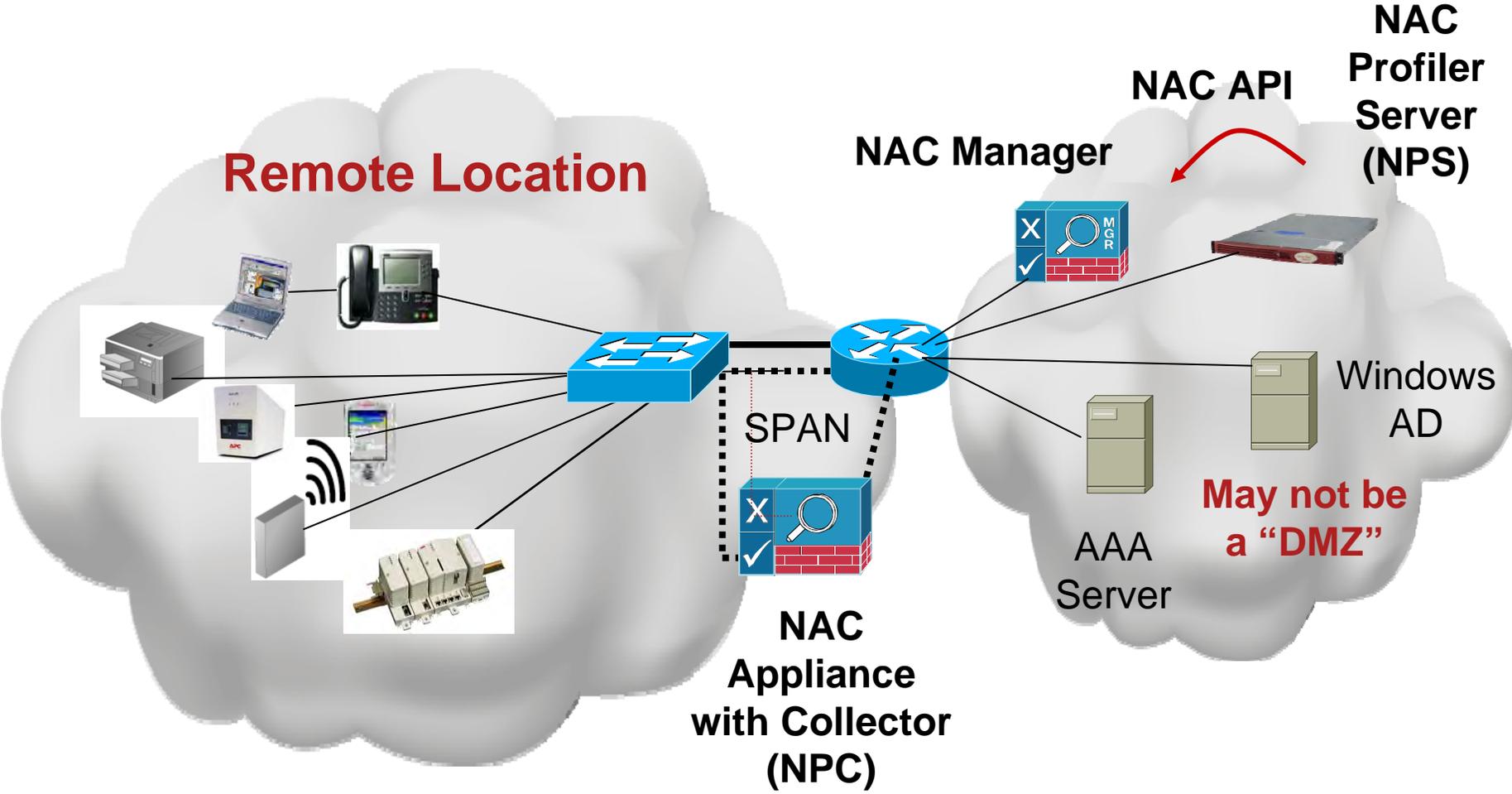
NAC Profiler Collector (NPC)

- Gathers information about the endpoints associated with that NAC Appliance (CAS)
- Information gathered includes data from SNMP, Network Traffic Analysis, and/or Active Profiling



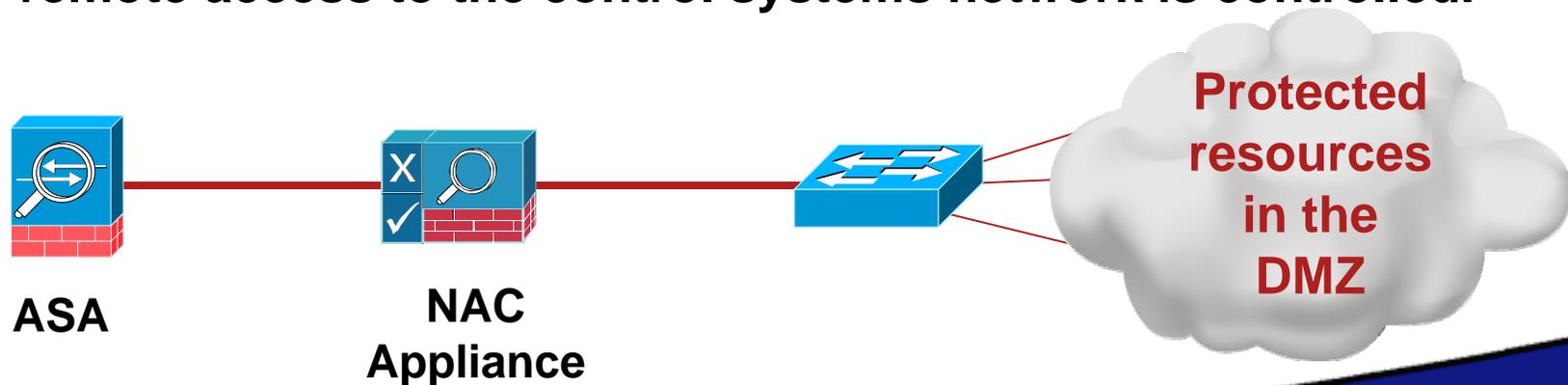
- Distributed Collector model allows many NPCs to work with a single NAC Profiler Server (NPS)
- NPC resides on NAC Appliance (CAS)

NAC Profiler and Collector



In-Band NAC Deployment for Remote Access

- ◆ NAC Appliance deployed in-line between ASA and Switch
- ◆ Remote users authenticate to ASA, e.g. via SSL VPN
- ◆ NAC Appliance then enforces user role by granting user access to appropriate VLANs and preventing access to others.
- ◆ This would be the NAC deployment model in the DMZ where remote access to the control systems network is controlled.



NAC Deployment Guidelines for IACS

◆ Profiler Guidelines

- Profile creation not trivial
- Easy when you have similar devices (ports, protocols)

◆ Architecture/Design Practice

- Out-of-band placement of the appliances (DMZ, Enterprise)
- In-band placement problems and lessons

◆ Others

- Cost issues
- Configuration

Agenda

- ◆ Risks and Benefits
- ◆ Secure Remote Access into an IACS
- ◆ Secure Local Access into an IACS
- ◆ Secure Direct Access enabled by NAC
- ◆ Summary

Key takeaways

- ◆ **Secure Access provides a clear value for organizations**
- ◆ **Different Secure Access options available to fit various needs**
- ◆ **NAC Enables Security for a Direct Access**

THANK YOU...