Security Frameworks

An Enterprise Approach to Security

Robert "Belka" Frazier, CISSP
belka@att.net

Security

- Security is recognized as essential to protect vital processes and the systems that provide those processes
- Security is not something you buy, it is something you do

What is Security?

- Security is no longer just controlling the perimeter or layered
- Transactions use all of the network, from DMZ to Database
- ALL of the network and resident systems have to be secured

What Securing All of the Enterprise Really Means…..

- Firewalls, routers, applications, passwords
- Intrusion detection – NIDS and HIDS
- Proactive scanning, pen testing
- System Configuration Monitoring – “Health Checking”
- VoiP, Wireless, Embedded Systems
- 24x7 Monitoring
- Analytical review and correlation
- Policies, Procedures, Personnel

What Is *Effective* Security

- Combination of appliances, software, alarms, and vulnerability scans working together in a well-thought out architecture
- Extends to policies, procedures, and people
- Monitored 24x7
- Designed to support the security goals of the Enterprise

The Security Framework

- The Security Framework is a coordinated system of security tools
- Similar to the Enterprise management framework
- Extends end to end of the customer enterprise architecture
- Security data centrally monitored 24x7 in a Security Operations Center
- Data analyzed using correlation tools

Security Framework Considerations

- Mapped to the customer’s architecture to provide end to end security
- Uses existing commercial and open source tools
- Leverages existing security infrastructure to quickly build out the security framework

Benefits of a Security Framework

- Provides Enterprise security that is :
  - Consistent
  - Constant
  - Covers everything
- Characteristics of Good Enterprise Security are:
  - Reliable
  - Robust
  - Repeatable

Benefits of a Security Framework
(continued)

- An Effective Security Framework is:
  - Monitored
  - Managed
  - Maintained
- This is the “raison d’être” for a Security Framework

Security Frameworks

Using the Framework Approach

Map Security Framework to Enterprise Architecture

- The Security framework follows structure of Open Systems Interconnect (OSI) 7-Layer Network Reference Model
    1. Physical
    2. Data Link
    3. Network
    4. Transport
    5. Session
    6. Presentation
    7. Application

Additional Layers of the Security Framework

- The security framework adds the financial and “political” layer (8 & 9)

The Security Framework -- Physical Layer

Physically secure and mange the cable plant

- Wiring closets
- WAN connections
- CSU/DSU

Physically secure and control access to networking equipment

- Routers
- Hubs
- Switches

Physically secure and control access to servers, mainframes

Provide redundant power and WAN connections

The Security Framework-- Data Link and Network Layers

- VPNs protecting the links between networks
- Network Intrusion Detection Systems (NIDS) watching traffic for attacks
- Host Intrusion Detection Systems (HIDS) protecting connections to critical servers/hosts
- Virus scanning taking place on traffic coming in from outside the customer’s network.

The Security Framework-- Network and Transport Layer

- Firewall performing stateful inspection of incoming and outgoing packets
- Router Access Control Lists (ACLs) filtering packets bound between networks
- Virus scanning of attachments at the e-mail gateways

The Security Framework-- Session, Presentation and Application Layers

- OS and application hardening at the system level
- Conduct security health checking to determine if security polices for types of applications allowed to run, password composition and length, services allowed on hosts, etc. are being followed
- Provide vulnerability scanning to test the configuration of applications and systems, looking for vulnerabilities, missing patches, etc.
- Conduct penetration tests to determine if machines can be exploited and privileged access gained

The Security Framework-- Presentation and Application Layers

- User account management on the network
- User account management on individual systems
- User account management for specific applications, RDBMS, etc.
- Virus scanning and updates on individual machines and user desktops
- Role & Rules Based Access Control (RBAC)
- PKI and digital certificates

The Security Framework-- Financial Layer

- Leverages existing security infrastructure to reduce costs
- Provides an operational framework for conducting regular security checks
- Lends itself to outsourcing to a managed security service provider
- New technologies can be incorporated into the security framework
- Security costs are easier to identify, budget, and control.

Security Framework– the “Political” Layer

- Provides a platform to align security with business goals just as enterprise system management normalizes the enterprise

- Framework is extensible to and modular, flexible to meet changing business objectives.

Security Frameworks

A More Detailed Technical Look

Mapping Security Framework Components to the Architecture

Security Component	Architecture Layer	Architecture Component Description
Service Delivery Center (SDC)	Layer 1 - Physical Layer	The Data Center controls physical cable pant connecting architecture together in a network. Provides physical security to networking components and hardware. Provides physical security to server hardware. Redundant power and WAN connections.
Virtual Private Networks (VPN)	Layer 2/3 – Data Link and Network Layers	VPN tunnels encrypt data flowing over the data link to protect it from outside scrutiny. Bit stream is encrypted, sent over the wire, and unencrypted at the far end.
Network Intrusion Detection (NIDS)	Layer 2/3 – Data Link and Network Layers	Monitor network traffic and system logs to compare what's happening in real-time to known methods of hackers. When a suspicious event is detected, an alarm is kicked off. In addition the Intrusion Detection system may suspend or drop the offending connection, all while recording as much information as possible
Host Intrusion Detection	Layer 2/3 – Data Link and Network Layers	HIDS Sensor scans bit streams as they reach the host system to match patterns and signatures that are indicative of an attack against the host or its applications. When a malicious pattern is detected the HID sends out an alert.

Mapping Security Framework Components to the Architecture

Security Component	Architecture Layer	Architecture Component Description
Virus Scanning	Layer 2 & 3 – Data Link and Network Layers	Virus canning software looks at bit streams flowing across data link to match signature patterns that indicate malicious code and viruses.
Firewalls and firewall appliances	Layer 3 & 4 – Network and Transport Layers	A device or software that blocks Internet communications access to a private resource. The resource can be a network server running a firewall as an application or an appliance with firewall application running as firmware.
Routers	Layer 3 & 4 – Network and Transport Layers	Use Cisco IOS to create access control lists (ACLs) to filter IP packets. ACLs on routers can shape traffic and restrict traffic flow between network segments. IP address schemes can segment the architecture by network, making ACLS and firewalls rules easier to manage.
Virus scanning of attachments	Layer 3 & 4 – Network and Transport Layers	Virus scanning software opens attachments entering and leaving the network to check for patterns and signatures the would indicate malicious code.

Mapping Security Framework Components to the Architecture

Security Component	Architecture Layer	Architecture Component Description
Legacy Access Control	Layer 5 – Session Layer for Legacy systems	Mechanisms used by legacy systems to control access to secure resources. These can include RACF, Top Secret, ACF2 and NT Domain Security. Legacy access controls can also be used as part of credential synchronization (single sign-on) systems.
OS & system Hardening	Layer 5, 6, 7 – Session, Presentation, Application Layers	Process of ensuring OS patches are up to date, unnecessary services are turned off, unneeded applications and tools are removed, and applications are patched.
Vulnerability Scanning	Layer 5, 6, 7 – Session, Presentation, Application Layers	Tool to scan for vulnerabilities, missing patches, new known vulnerabilities and exploits. Tools are updated regularly from CERT advisories, bug lists, and new exploit notices.
Vulnerability Assessment	Layer 5, 6, 7 – Session, Presentation, Application Layers	Team of trained ethical hackers attempt to gain access to target machine, simulating a real world attack as a malicious intruder would to test the security architecture.

Mapping Security Framework Components to the Architecture

Security Component	Architecture Layer	Architecture Component Description
User account management on the network	Layers 6 & 7, Presentation and Application Layers	Managing user accounts on and access to the network. Uses Network NOS, Active Directory, LDAP, etc. to authenticate.
User account management on systems	Layers 6 & 7, Presentation and Application Layers	User account management on individual system. Management of privileged accounts, separation of duties between administrators
User account management on applications	Layers 6 & 7, Presentation and Application Layers	Manage access to software and applications such as RDBMS, etc.
Virus scan engine and signature updates	Layers 6 & 7, Presentation and Application Layers	Updates to anti-virus applications, scan engines, virus signatures, etc.

Mapping Security Framework Components to the Architecture

Security Component	Architecture Layer	Architecture Component Description
PKI & Credential Management	Layer 6 & 7 – Presentation and Application Layers	Provides capabilities for the management of user credential information. This information can be a user id, password, PKI, digital certificate or biometric information.
Role Based Access Control (RBAC)	Layer 6 & 7 – Presentation and Application Layers	The security engine responsible for definition and decision making around all security policies. Applications delegate security decision making to the security engine. This delegation occurs through existing security extension points within the application domain. Security is seamless and non-intrusive from the application's point of view
Security Operations Center (SOC)	Layer 8 - Financial Layer	24 x 7 security management using SOC to manage and monitor security architecture. Ensures real time monitoring of the security of the network.

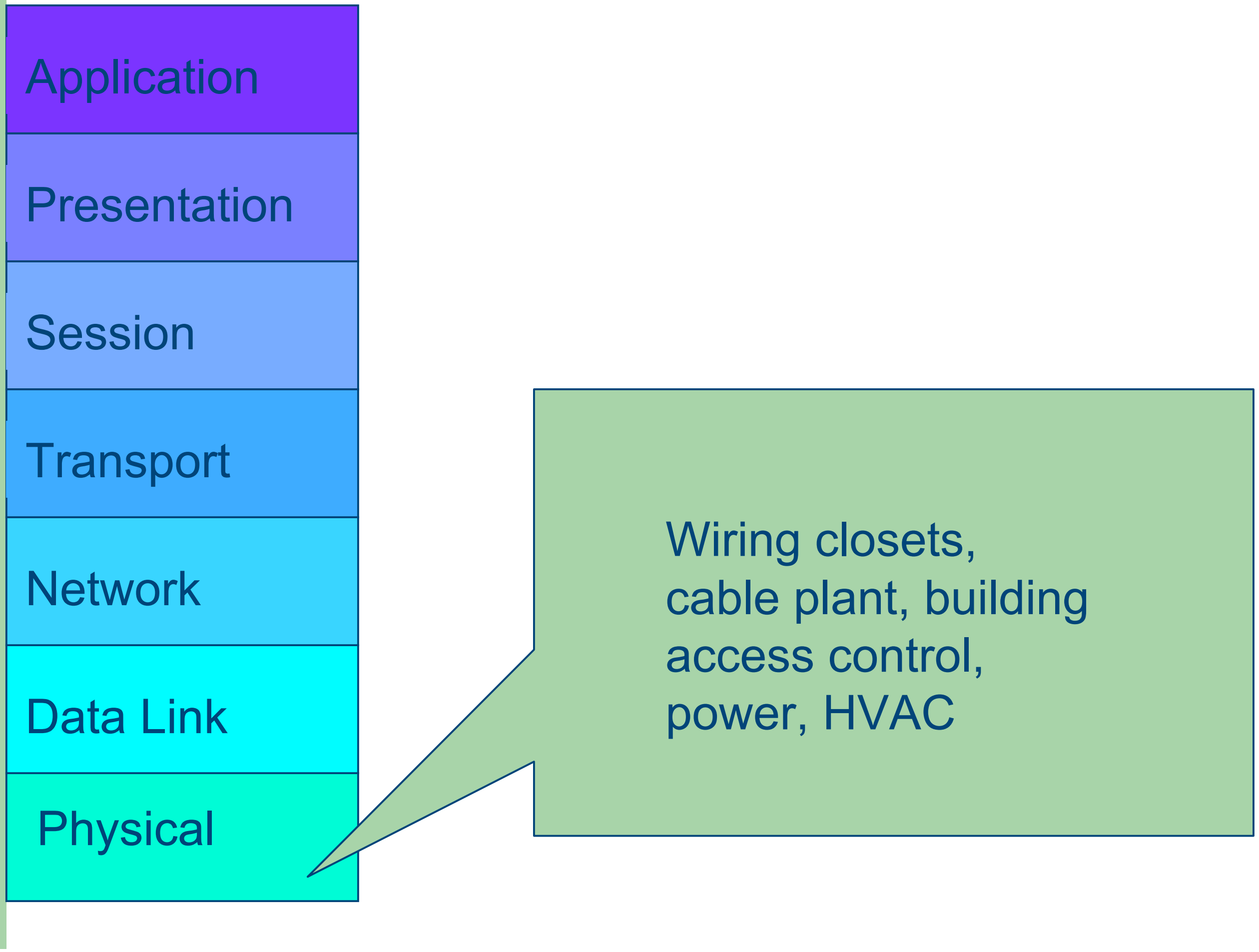
Mapping Security Framework Components to the Architecture

Security Component	Architecture Layer	Architecture Component Description
Using Existing Security Infrastructure	Layer 8 – Financial Layer	Security tools, connections, trained personnel are leveraged to provide security services and build a security framework for less than the cost to duplicate the same services as point security solutions
Provides an operational framework for regular security checks	Layer 8 – Financial Layer	Security becomes part of the enterprise operations, providing consistent security management in the same fashion as enterprise system management. In the same way, the security framework reduces the total cost of security.
Lends itself to outsourced managed security services	Layer 8 – Financial Layer	A security framework can be implemented by using managed security services that build, monitor, and manage security across the enterprise.

Mapping Security Framework Components to the Architecture

Security Component	Architecture Layer	Architecture Component Description
Extensible to new networks and technologies	Layer 8 – Financial Layer	As network grow and merge, the framework can extend into these new segments. New technologies such as wireless, VoIP, smart HVAC systems can also be managed and monitored by the security framework.
Security cost are more predictable	Layer 8 – Financial Layer	The cost of providing security becomes more predictable and manageable. Security costs are consolidated into the framework, facilitating budget and planning.
Provides a platform to align security with business goals	Layer 9 – Political Layer	Security framework can be used to manage security consistently to meet business goals just as the enterprise system management manages the IT infrastructure to meet the company objectives.
Security Framework is modular, quickly extensible	Layer 9 – Political Layer	If new technology such as wireless networks are adopted, security controls can be added to the framework to manage the new initiatives. Networks added through acquisitions can be quickly added to the security framework.

Security Framework by Services



Application

Presentation

Session

Transport

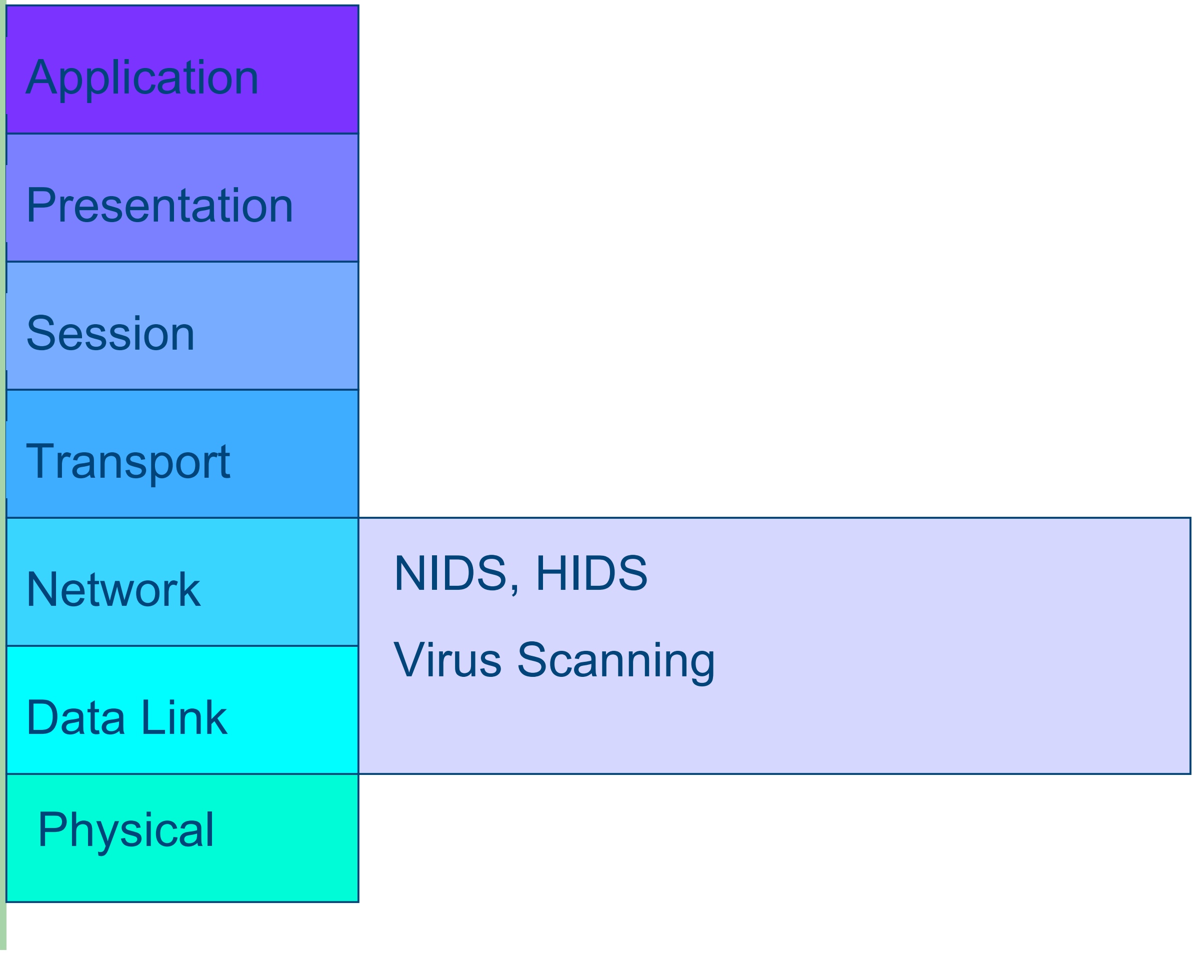
Network

Data Link

Physical

Wiring closets,
cable plant, building
access control,
power, HVAC

Security Framework by Services



Application

Presentation

Session

Transport

Network

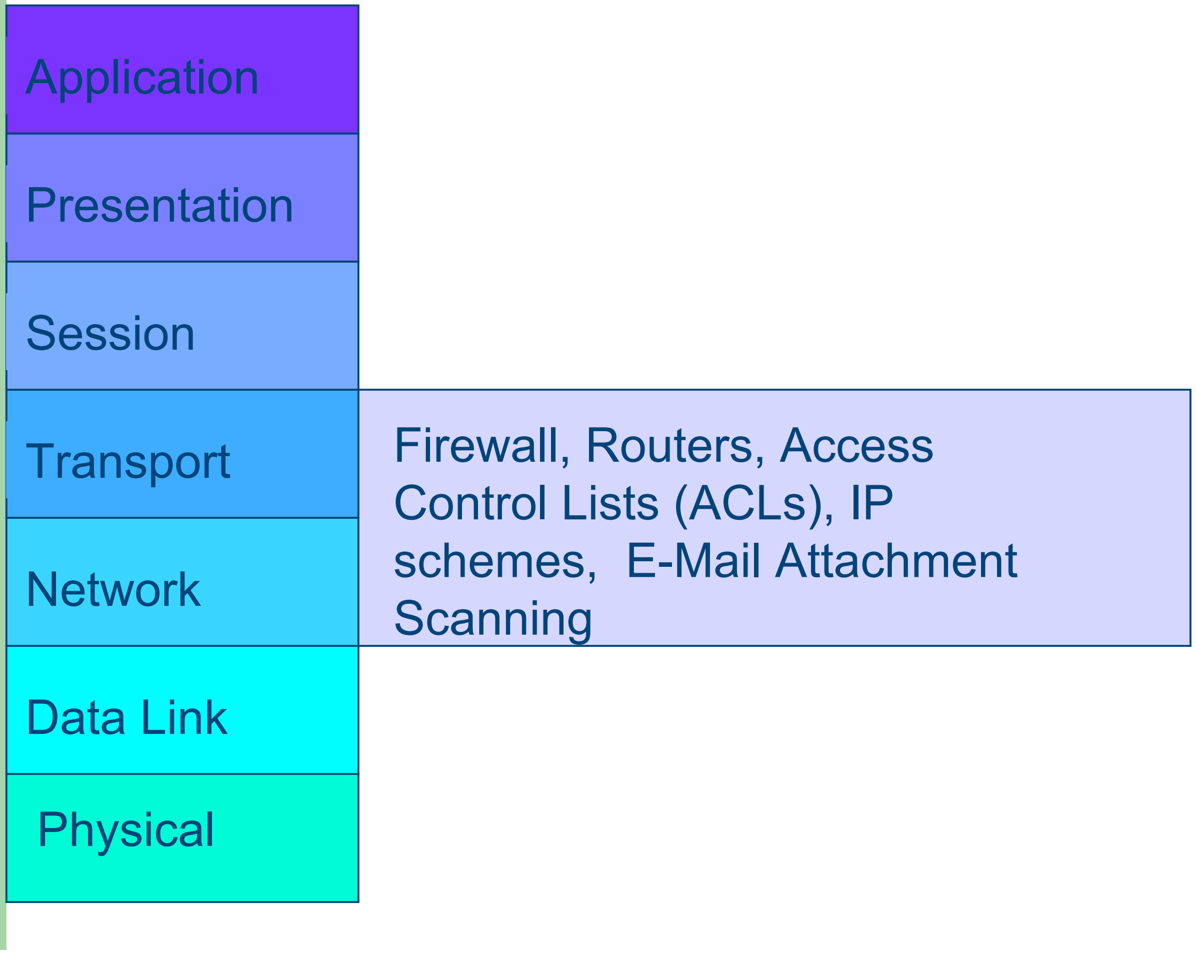
Data Link

Physical

NIDS, HIDS

Virus Scanning

Security Framework by Services



Application

Presentation

Session

Transport

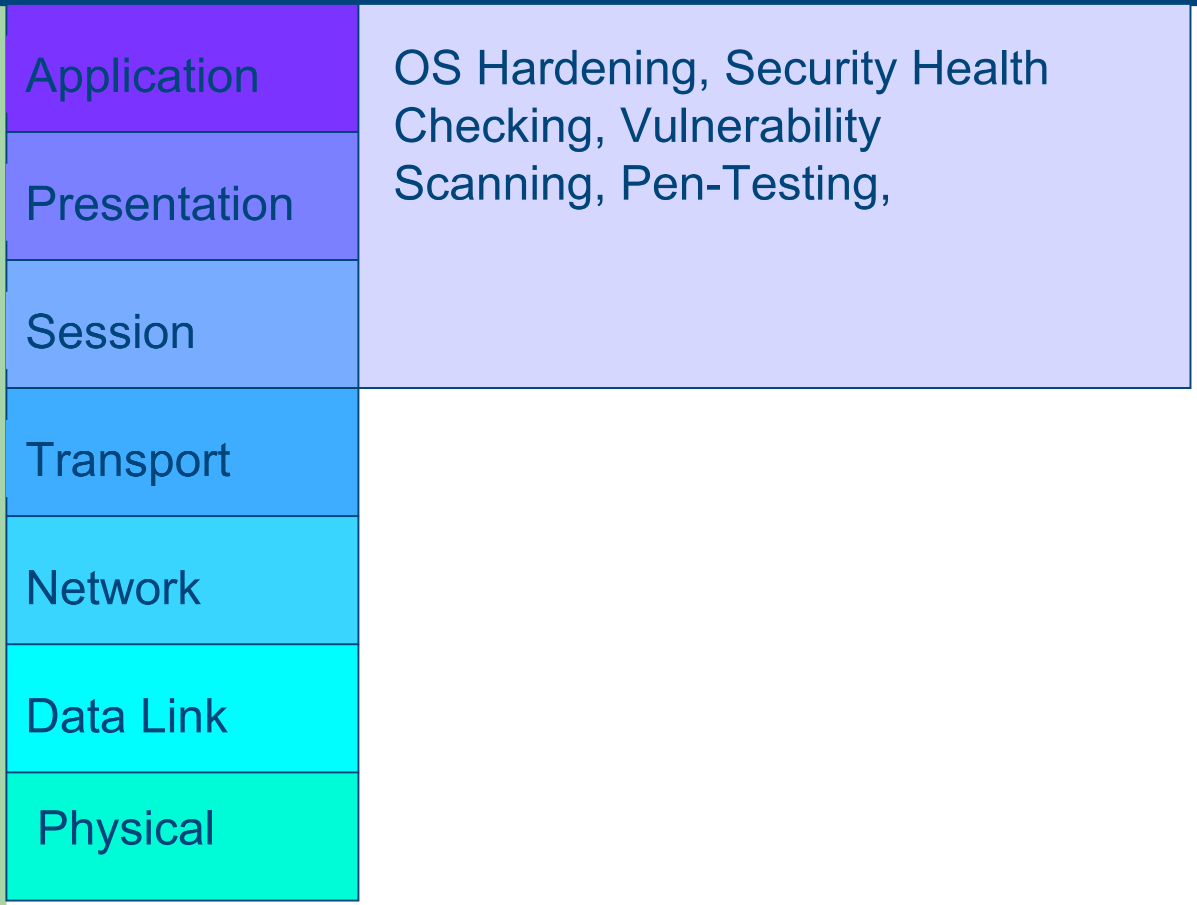
Network

Data Link

Physical

Firewall, Routers, Access Control Lists (ACLs), IP schemes, E-Mail Attachment Scanning

Security Framework by Services



Application

Presentation

Session

Transport

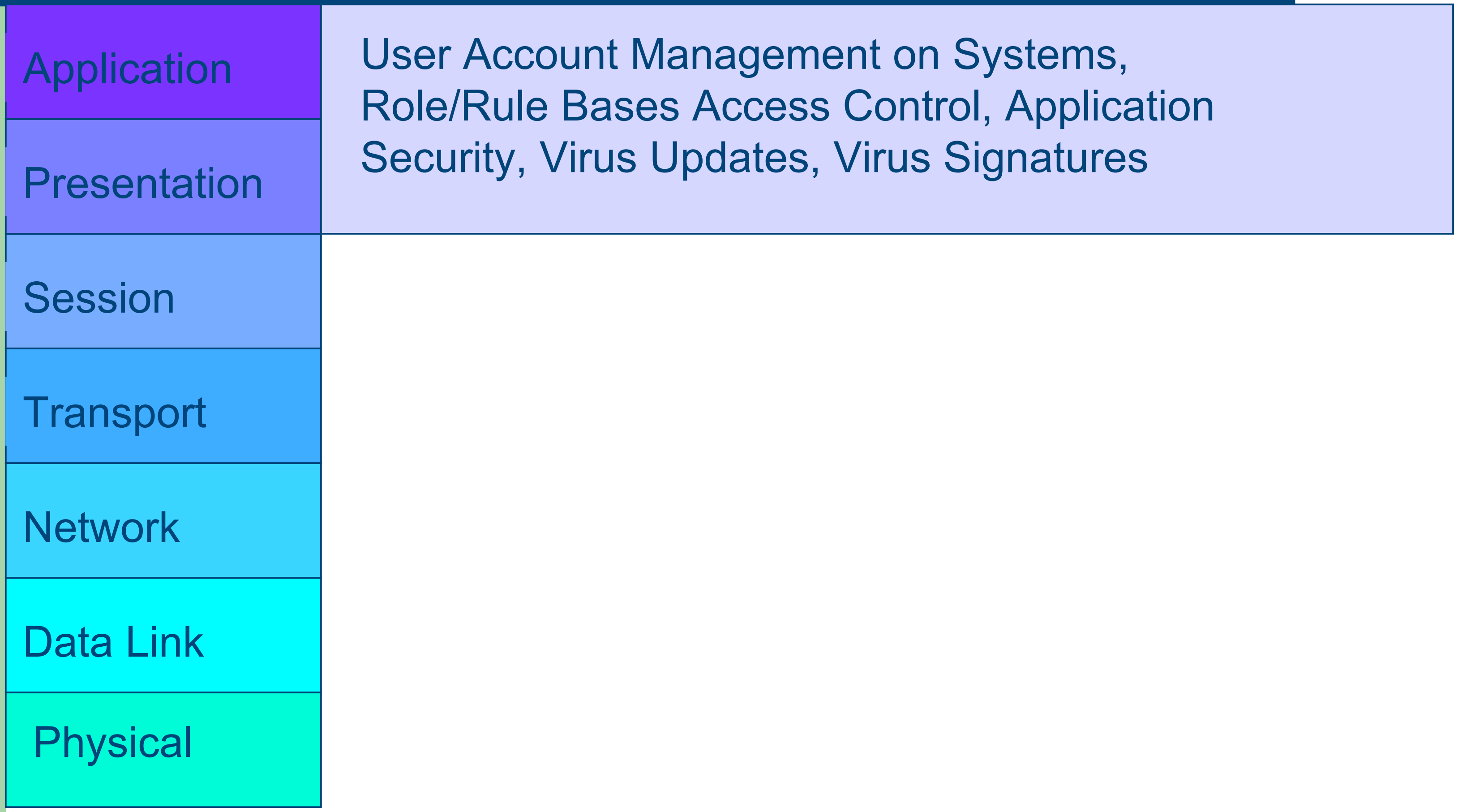
Network

Data Link

Physical

OS Hardening, Security Health Checking, Vulnerability Scanning, Pen-Testing,

Security Framework by Services



Application

Presentation

Session

Transport

Network

Data Link

Physical

User Account Management on Systems, Role/Rule Bases Access Control, Application Security, Virus Updates, Virus Signatures

Security Frameworks - Summary

- To sum it all up
  - Security Frameworks provide end to end security – from the DMZ to the Database
  - Security is managed and monitored consistently and continually
  - The security framework becomes the technology that turns security policies into practice
  - New technologies and new networks can plug into the security framework
  - Security costs become more predictable and manageable

Security Frameworks – More Q/A

- Questions?