FHDA Network/Security Architecture

Management Overview

Ken Agress
Senior Consultant, NTS

Fred Cohen
Senior Consultant, SRMS

Agenda

Introduction & Background

What is a Network/security Architecture?

Why Have an Architecture?

The Burton Group Architecture Process

The FHDA Architecture

Key FHDA Issues

- Security
- Network

Conclusion

Q&A and Discussion

Agenda

Introduction & Background

What is a Network/security Architecture?

Why Have an Architecture?

The Burton Group Architecture Process

The FHDA Architecture

Key FHDA Issues

- Security
- Network

Conclusion

Q&A and Discussion

Introduction & Background

Introductions

Project Background

- Why did we do this project?
- Who was involved?
- What were the deliverables?
- How will this be used?

Why Burton Group?

Agenda

Introduction & Background

What is a Network/security Architecture?

Why Have an Architecture?

The Burton Group Architecture Process

The FHDA Architecture

Key FHDA Issues

- Security
- Network

Conclusion

Q&A and Discussion

What is a Network/Security Architecture?

An architecture is a forward-looking document that:

- Defines how an organization will approach technology decisions
- Describes specific requirements and goals that technology must address to meet the organization's needs
- Establishes standards that can be leveraged in a useful fashion over a long period of time
- Allows IT to evaluate solutions in a neutral and unbiased fashion

An architecture is not:

- A design that describes the environment with specificity
- A detailed description of configurations or devices
- A list of products, vendors, solutions, or systems that will be implemented

Agenda

Introduction & Background

What is a Network/security Architecture?

Why Have an Architecture?

The Burton Group Architecture Process

The FHDA Architecture

Key FHDA Issues

- Security
- Network

Conclusion

Q&A and Discussion

Why Have an Architecture?

An architecture allows an organization to:

- Reduces the complexity of managing and operating the environment.
  - Reduction in cost, operational issues
  - Improved consistency and greater effectiveness
- Define a set of technology standards that:
  - Can be applied to a wide range of technical solutions
  - Provide for interoperability of hardware/software
  - Ensure required needs are addressed
  - Support bid specifications that are targeted and meet the needs
- Describe approaches to technology that the district can review and re-visit as requirements or technologies change
- Develop processes and procedures based on a common understanding of technical and business requirements.

An architecture is intended to be a “living document” that is revisited regularly and modified over time.

Agenda

Introduction & Background

What is a Network/security Architecture?

Why Have an Architecture?

The Burton Group Architecture Process

The FHDA Architecture

Key FHDA Issues

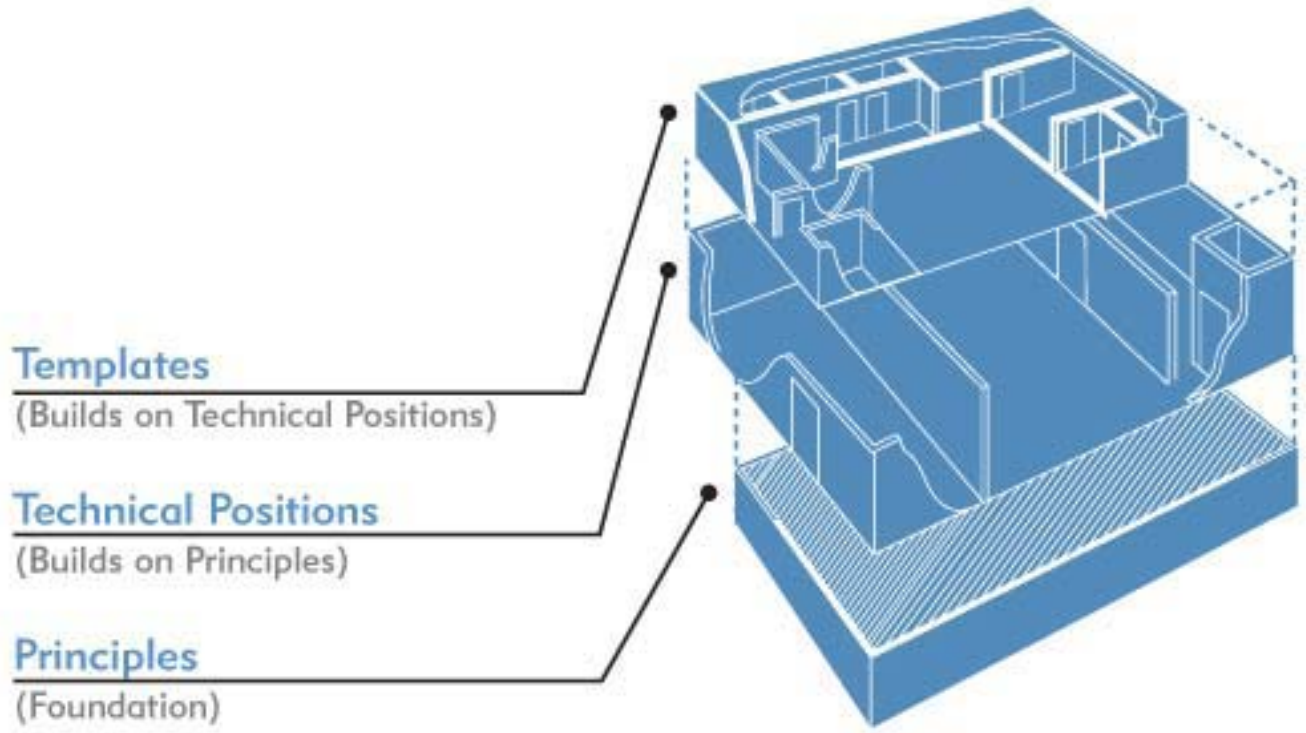
- Security
- Network

Conclusion

Q&A and Discussion

The Burton Group Architecture Process

Burton Group leverages a structured methodology to assist clients.



Business needs determine the specific goals, this process defines the standards.

The Burton Group Architecture Process

What we did:

- Gathered background data through interviews and document review
- Discussed technical and business needs with FHDA personnel
- Conducted a one week workshop to create the architecture with FHDA management and staff
  - Described FHDA Principles
  - Defined FHDA Technical Positions
  - Created FHDA Templates
- Prepared and presented the resulting architecture

What FHDA needs to do:

- Socialize the architecture within the district
- Perform annual reviews of the architecture
- Understand the gaps, prioritize them, and act on them
- Develop standard processes that leverage the architecture

Agenda

- Introduction & Background
- What is a Network/security Architecture?
- Why Have an Architecture?
- The Burton Group Architecture Process
- The FHDA Architecture
- Key FHDA Issues
  - Security
  - Network
- Conclusion
- Q&A and Discussion

FHDA Key Business Drivers

- Support the district's education objectives
  - Distance learning
  - "Anywhere/anytime access"
- Improve support for key applications:
  - EIS System
  - Multicast for audio/video services
  - Prepare for PBX replacement
- Support a range of users effectively providing:
  - Improved bandwidth, reliability, protection
  - Support for many different types of traffic
- Build network in a cost effective, sustainable, adaptable fashion

The FHDA Architecture

What does FHDA get out of this Architecture?

Properly secured, reliable communications

for students, faculty, and staff

that adapts as requirements change.

The FHDA Architecture: Wireless

Enhanced wireless access is called for:

- Wireless standards with greater range, bandwidth
- Ability to provide support for different user groups on a single infrastructure
- Security appropriate to the type of user and group
- Guest access where allowed

The FHDA Architecture :Multimedia

The standards adopted provide support for:

- Streaming video and audio
- Multicast applications such as video conferencing, video distribution, and broadcasting
- Increased bandwidth to support new and interesting types of media
- Proper classification and handling of different types of traffic
- Support for IP Telephony as a potential PBX replacement

The FHDA Architecture: Proactive Management

The architecture will help ETS achieve:

- Enhanced management capabilities and visibility into network performance and conditions
- Greater understanding of applications and services the network should support
- Improved historical tracking for trend analysis and capacity planning
- Process and procedure improvements to standardize responses, reduce “heroic efforts”
- Uniform approaches to technical issues, problem identification, prioritization, and resolution

The FHDA Architecture: Improved Access

The architecture adds:

- Support for properly secured, authorized “anytime/anywhere” access
  - Student access to resources and materials
  - Faculty access to systems and services
  - Staff access for administrative purposes
  - 3rd parties supporting FHDA
  - Green initiatives for facilities management
- Higher performance core network
- Faster, more capable connections between buildings & locations

Agenda

Introduction & Background

What is a Network/security Architecture?

Why Have an Architecture?

The Burton Group Architecture Process

The FHDA Architecture

Key FHDA Issues

- Security
- Network

Conclusion

Q&A and Discussion

Security Architecture Key Issues

The situation today:

- No IT risk management function
- Content, applications, and systems are not adequately inventoried
- Processes are not well defined or automated
- Lack of structure for controls
- Detection of security related events is inadequate to the need

Security: No Risk Management Function

What is the problem?

- For information and information technology no risk management function is in place for FHDA

Why does it matter?

- Without this function, rational decision-making cannot be done regarding what to protect and how well.

How can it be solved?

- Someone has to be put in charge of performing this function for the district.
- They need the skills, knowledge, and tools to do it.
- Until this is done, design decisions may be seen as without a rational basis and justification

Security: No Inventory of Content and Systems

What is the problem?

- There is no comprehensive inventory of content, applications, and systems
  - What do they do?
  - How do they do it?
  - What are they for?

Why does it matter?

- If you don't know what you have:
  - How do you know how to protect it?
  - How do you know when you are done?
  - How do you know how well you have done it?

How can it be solved?

- Generate an inventory over time
  - Start with what's obvious and critical – keep going
  - Over time, inventory all new things, systematically deprecate what's not inventoried till done

Security: Processes Not Well Defined

What is the problem?

- The processes for getting things done with content and technology are not systematically defined and consistently applied

Why does it matter?

- Processes are hard to repeat, depend on heroic effort of individuals, and are not well documented even after they have taken place.
- As complexity rises, so do costs, unless you systematize and automate functions

How can it be solved?

- Move toward a higher level of maturity in processes
- Add automation to support the effort

Security: Lack of Structure for Controls

What is the problem?

- Controls, where they exist, are ad-hoc and unstructured.

Why does it matter?

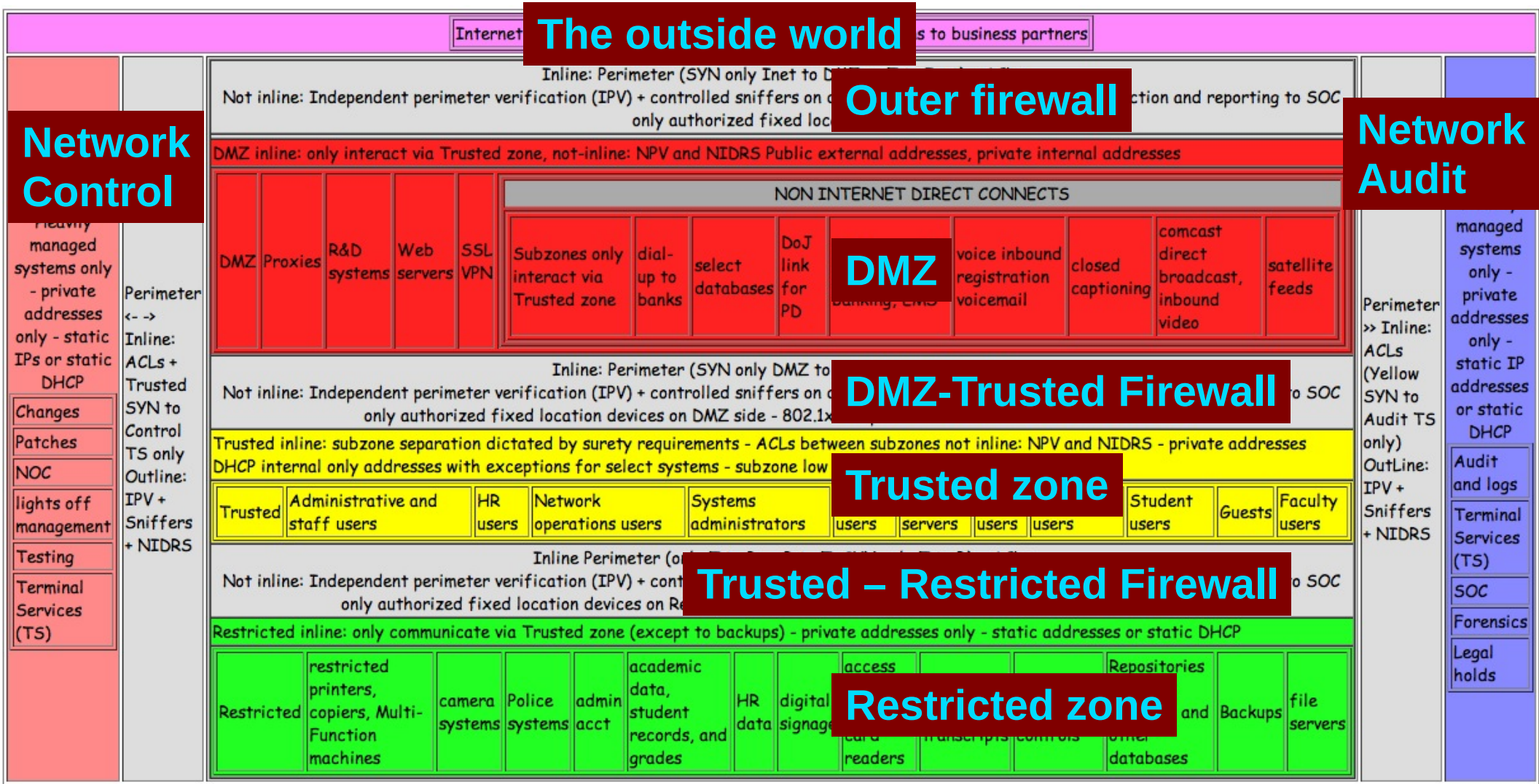
- It takes a lot of individualized effort to examine each item one at a time, therefore:
  - Many things are not examined
  - Many things are poorly controlled or not controlled at all.
- The cost of controls is far higher
- Economies of scale are not readily attainable.

How can it be solved?

- Structures should be put in place to allow content, applications, systems, and users to be controlled by common mechanisms based on defined characteristics. To wit:

Security: The Big Picture - Zones

Without drilling into the details...



Security: Detection Inadequate to the Need

What is the problem?

- You can't tell if you are being attacked or if you are misconfigured

Why does it matter?

- No passive defense can hold out forever.
- To defend you must detect and react in time to prevent potentially serious negative consequences (PSNCs) in excess of management specified thresholds (MSTs).
- If you can't detect, you can't react in a timely fashion.

How can it be solved?

- You need a systematic approach to detection of event sequences that can produce PSNCs – and MSTs.

Network: VLANs and IP

What's the problem?

- Existing IP addressing and VLAN schemes aren't capable of meeting business requirements

Why does it matter?

- Can't create a scalable network
- Can't support zones adequately
- Can't provide improved access

How can it be solved?

- Develop initial plans for new IP addressing
- Determine how and where VLANs will be leveraged
- Work with implementation team(s) to finalize and deploy

Network: Dynamic Computer Placement

What's the problem?

- FHDA needs to place users in the proper area of the network

Why does it matter?

- Users may receive too much/too little access
- Implementation could be overly complex and difficult to support

How can it be solved?

- Carefully plan implementation to minimize support burden
- Protocols and systems used (802.1x and Identity Management) will require careful, strategic consideration
- Strategy must be developed to some extent for use in bid documents

Network: Routing Priorities

What's the problem?

- Security standards require that traffic is inspected at appropriate points, which requires proper routing

Why does it matter?

- FHDA can't comply with the standards adopted without proper inspection, detection, and action

How can it be solved?

- Develop initial plans for routing through the network
- Work with implementation teams to finalize
- Test implementation prior to acceptance
- Regularly test routing to verify compliance

Network: Quality of Service

What's the problem?

- Different services demand different performance from the network
  - Telephony
  - Video conferencing
  - Video streaming
  - E-mail, browsing, other "standard" applications.

Why does it matter?

- Negative impact on quality for high-demand services
  - Can I make a connection?
  - Is the connection good enough?
  - Can I maintain the connection?

How can it be solved?

- Leverage application/content inventory to classify services
- Determine service requirements
- Define classification and enforcement mechanisms
- Create procedures that include characterization of new applications

Agenda

Introduction & Background

What is a Network/security Architecture?

Why Have an Architecture?

The Burton Group Architecture Process

The FHDA Architecture

Key FHDA Issues

- Security
- Network

Conclusion

Q&A and Discussion

So What's Next?

- Communicating the architecture throughout the district
- Translating the architecture into an effective design
- Regularly reviewing the architecture and updating as required
- Applying the architecture systematically and effectively

Conclusion

FHDA's Network/Security architecture is an important first step towards achieving:

Properly secured, reliable communications

for students, faculty, and staff

that adapts as requirements change.

FHDA can leverage the architecture because:

- It defines standards in a useful, modular fashion
- It provides the basis for decisions and allows discussion of priorities
- It describes a future state with identified gaps and action items

What questions do you have?