



Enterprise Firewall Protection Profile

Development Plan & Status Update

11th International Common Criteria Conference
Antalya, Turkey 24 September, 2010

Tom Price – Cisco Systems
Jane Medefesser – Juniper Networks

Introduction

- History of the Effort
- Old Paradigm vs. New Paradigm
- Structures and Features of the PP
- Future Schedule



Community Effort

Participants

- GOVT: NIAP, CESG, CSE
- PP Dev: Mitre, Aerospace
- Vendor: Cisco, Juniper, Microsoft, McAfee

Observers

- GOVT: BSI, DSD, Turkey, France, Sweden, Singapore
- Vendor: Fortinet, Intel, Checkpoint, ICSA

Goals



Consistent Results

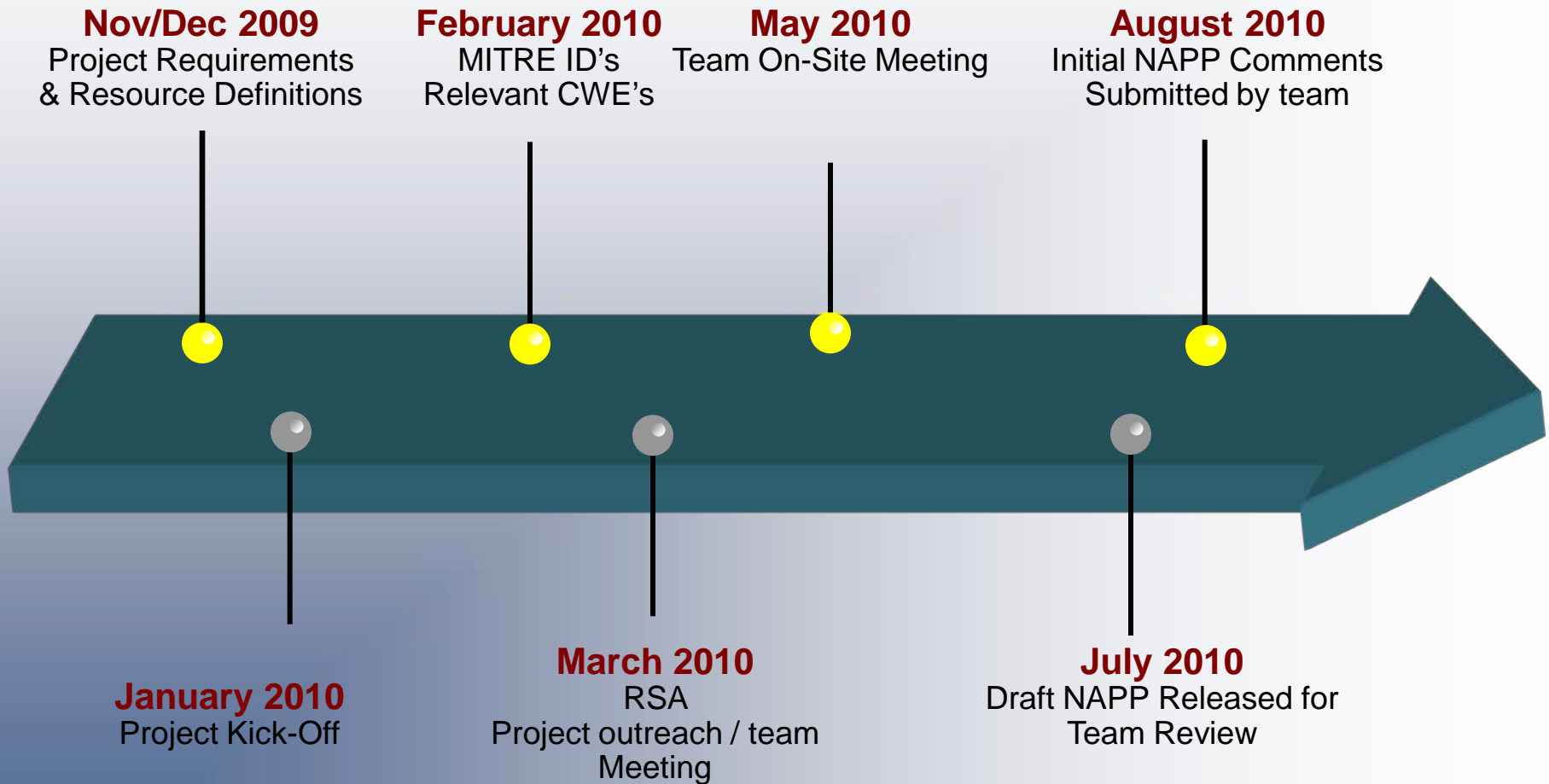
Simplified Testing

Meaningful Functional
Requirements

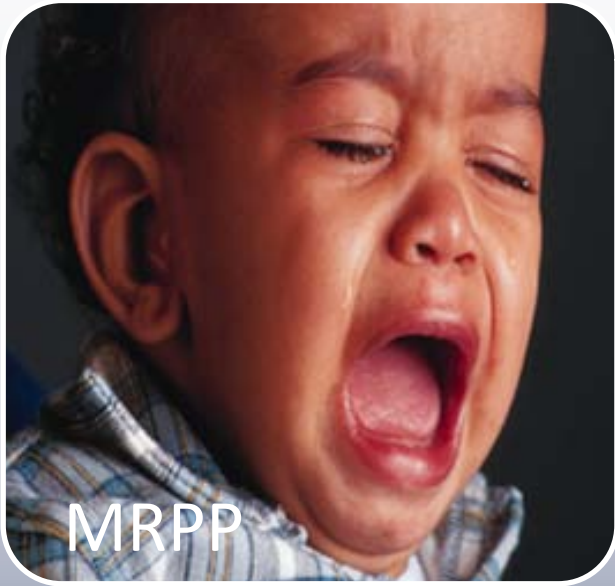
Certify Products
More Quickly

Continued Improvement
Through Ongoing Review

FWPP Background



What Makes It Different



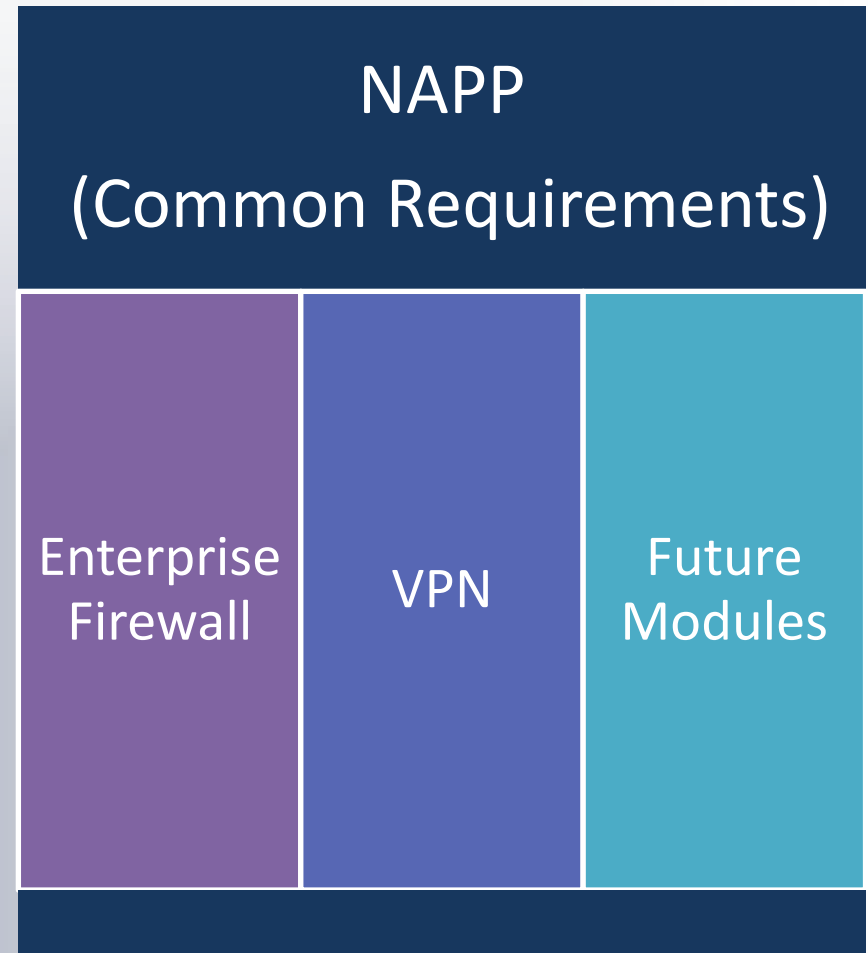
- Documentation Focused Evaluations
- Generic/Subjective Testing Reqs. (SARs)
- Created/Maintained by NIAP



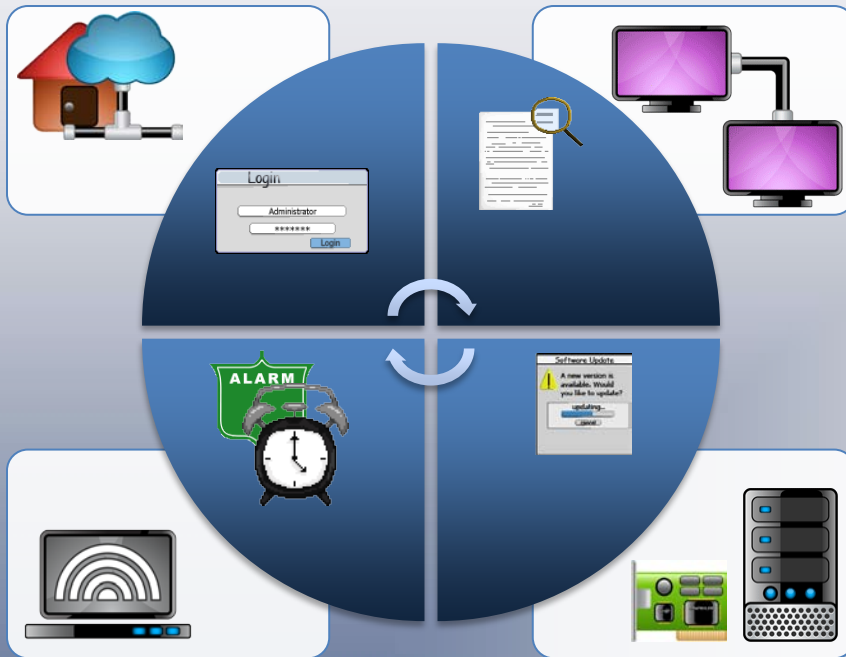
- Feature Focused Evaluation
- Relevant Technology Specific FSPs
- Community Based Creation & Maintenance

Modular Design

- Network Appliances PP
 - Common Requirements for all connected devices
 - Default PP for networking Security Target design
- Enterprise Firewall
 - Functional Requirements based on the needs of Enterprise deployments
 - Delta set to the NAPP
- VPN, Future Modules
 - Will follow same design



Network Appliance PP



Applicable to a wide array of products

- Any network connected Product
- Not tied to any technology type

Meaningful Functional Requirements

- Protected Communications
- Audit, Alarms, System management
- Identification & Authentication, etc.

Simplified Assurance Requirements

- Evaluator focus on weakness areas
And testing results

Firewall Functional Requirements

OLD

- Targeted at Many Use-Cases
- Static/Rarely Changing Requirements
- NIAP Developed
- Addresses General & FW Requirements

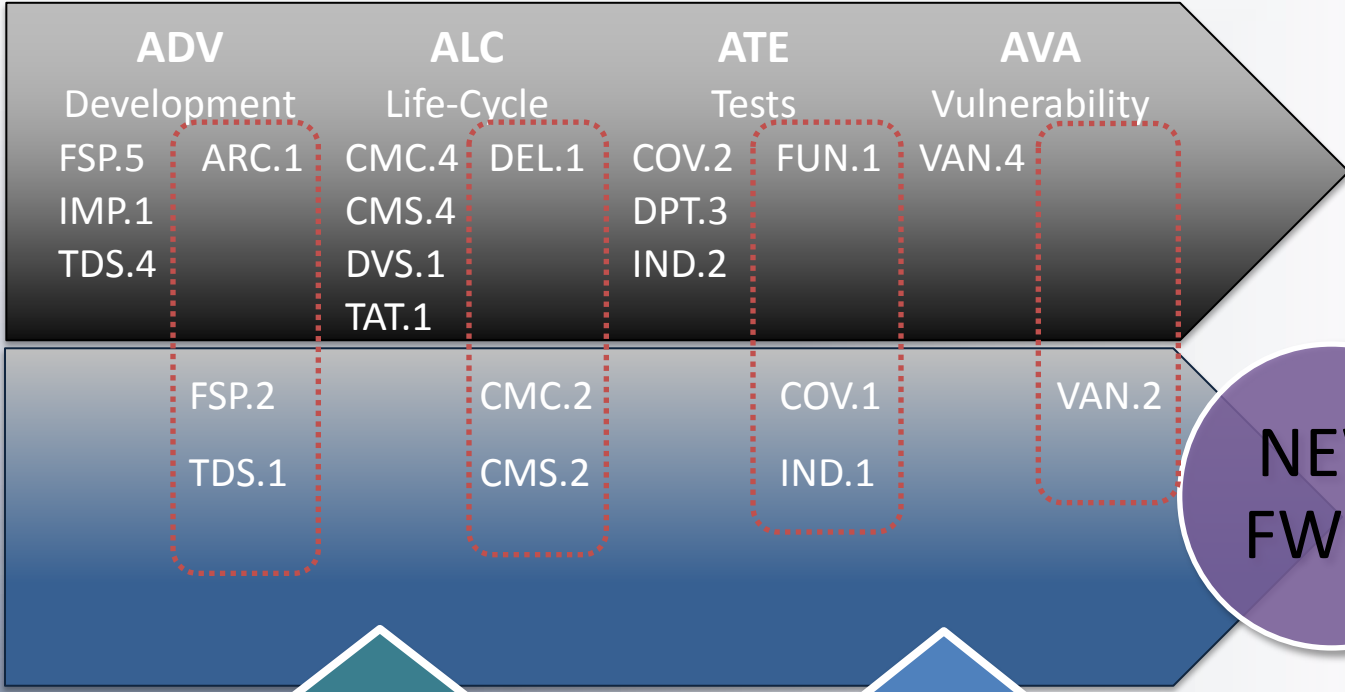
NEW

- Targeted for Enterprise Level Use-Cases (focused)
- Regularly Updated for relevance
- Community Developed
- FW Focused Requirements



Firewall Assurance Requirements

MRPP



NEW FWPP

Leveraged Crypto Conformance

Publicly Attest-able Results

Protection Profile Inputs

Vulnerability
Analysis

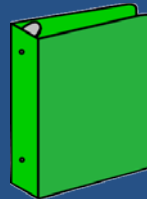
SANS Top-25
CWE, CVE

Deployment

CC V3.1
FIPS140-2

CCI
SCAP

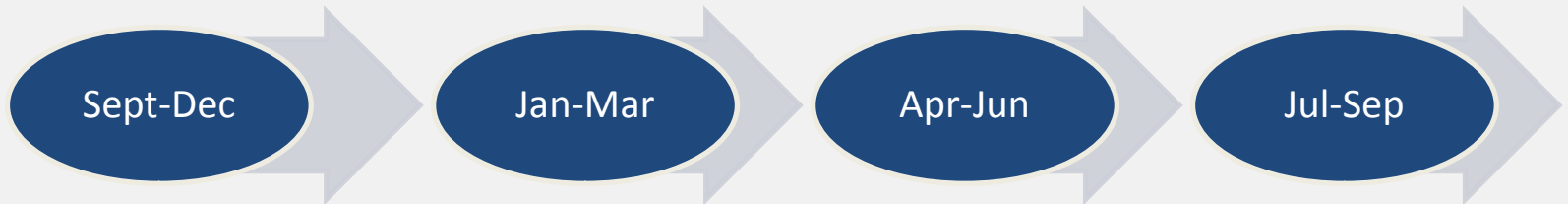
Standards



PP

High Level Schedule

Timeline



Milestones

9/2010 – Project Review
10/2010 – 1st Gen NAPP
11/2010 – Work group
Offsite

1/2011 – Project Review

5/2011 – Draft FWPP
& 2nd Gen NAPP

7/2011 – 2nd Gen NAPP
7/2011 – Enterprise FWPP

Deliverable



Immediate Next Steps

Three (3) sub-groups to provide planning, research and feedback to be used as input for the PP

Functional Capabilities

- Develop additional functional requirements for 2nd gen NAPP and Enterprise FWPP

Implementation and Design Weakness Mitigation

- Develop content based on software design & development practices which minimize weakness

Deployment and Operational Configuration

- Develop PP content based related to deployment and secure operation on the product

TEAM LEAD

Jane Medefesser
janem@juniper.net

TEAM LEAD

Tony Busciglio
abusigli@cisco.com

TEAM LEAD

Mike Grimm
mgrimm@microsoft.com

Would you like to Participate?



Summary / Conclusions

- New, Improved Development Paradigm
- Community Effort
 - Government & Industry Working Together
- Less Documentation
- Focused Functional and Assurance Requirements
- Work In-Progress
 - Target Publish Date 07/2011
- Participation is Welcome and Encouraged

Questions ?

Presentation Comments: *janem@juniper.net or tompric@cisco.com*

Google Group Inquiries: *<http://groups.google.com/group/firewall-pp>*

