Sun Ray Deep Dive

Sun Ray +
Solaris +
Trusted Extensions...

...*it's a SNAP!*

Matt Hatley
Desktop Technical Specialist
Sun Fed

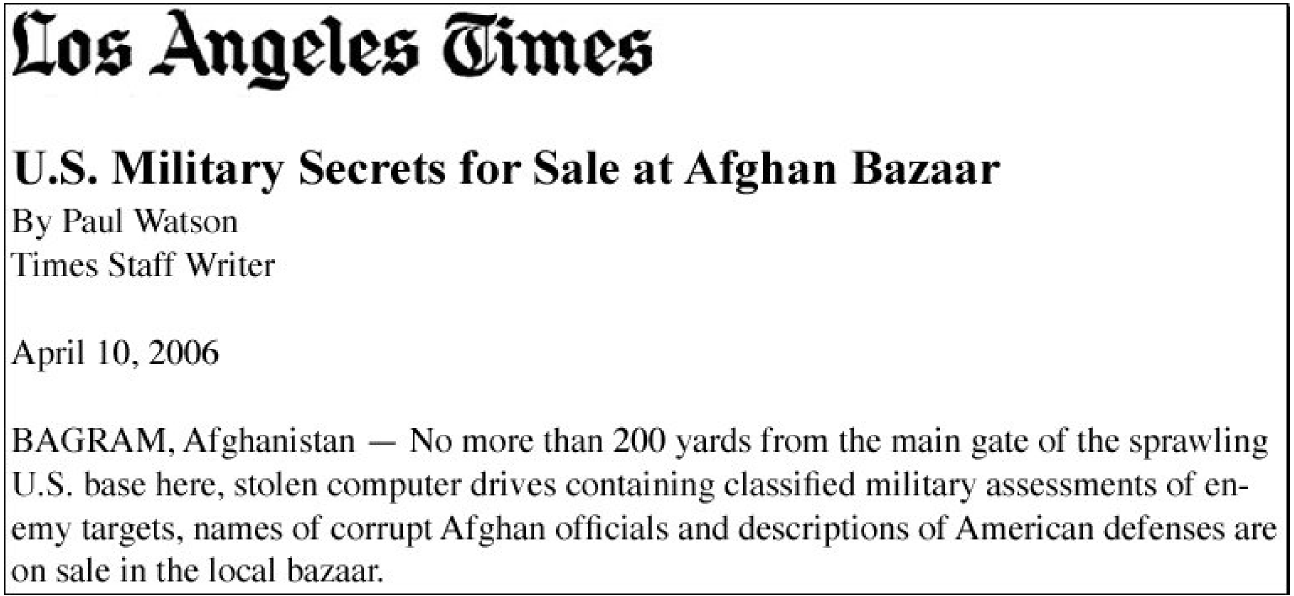
Agenda: S – N – A – P

Secure Network Access Platform

- Why You Should Care
- Basic Problem The Solution Solves
- What it is & How It Works
- What's unique about Sun Ray on TX
- Q&A, Demonstrations Throughout!

- SNAP is a Reference Architecture, not a product.

Why care about SNAP?



Los Angeles Times

U.S. Military Secrets for Sale at Afghan Bazaar

By Paul Watson
Times Staff Writer

April 10, 2006

BAGRAM, Afghanistan — No more than 200 yards from the main gate of the sprawling U.S. base here, stolen computer drives containing classified military assessments of enemy targets, names of corrupt Afghan officials and descriptions of American defenses are on sale in the local bazaar.

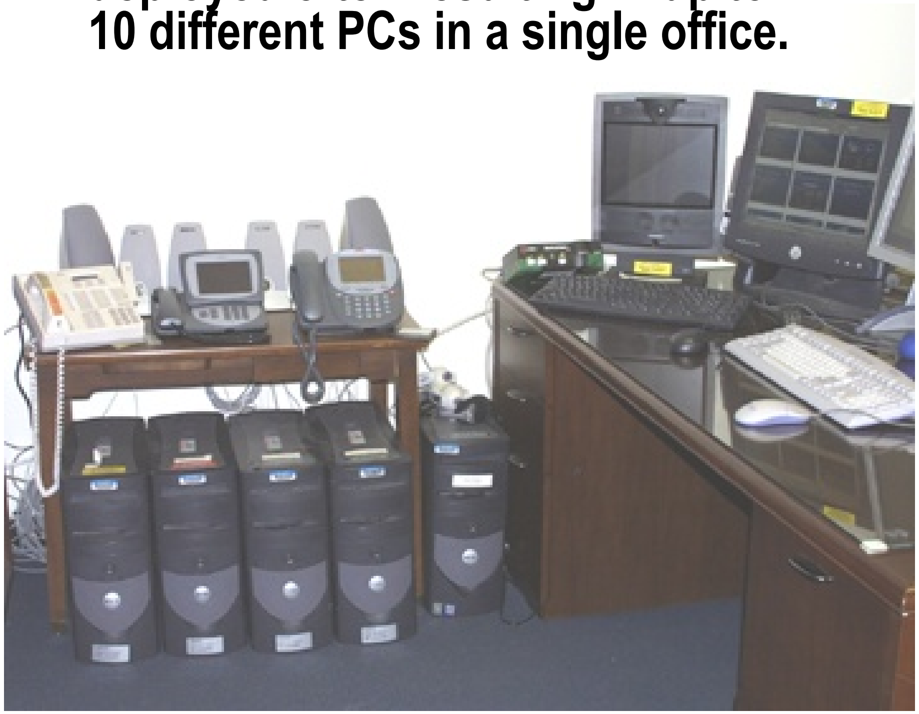
Because it **protects** & **centralizes** control of your data.

And it helps you avoid CNN moments like these!

SNAP Solves This Basic Problem...

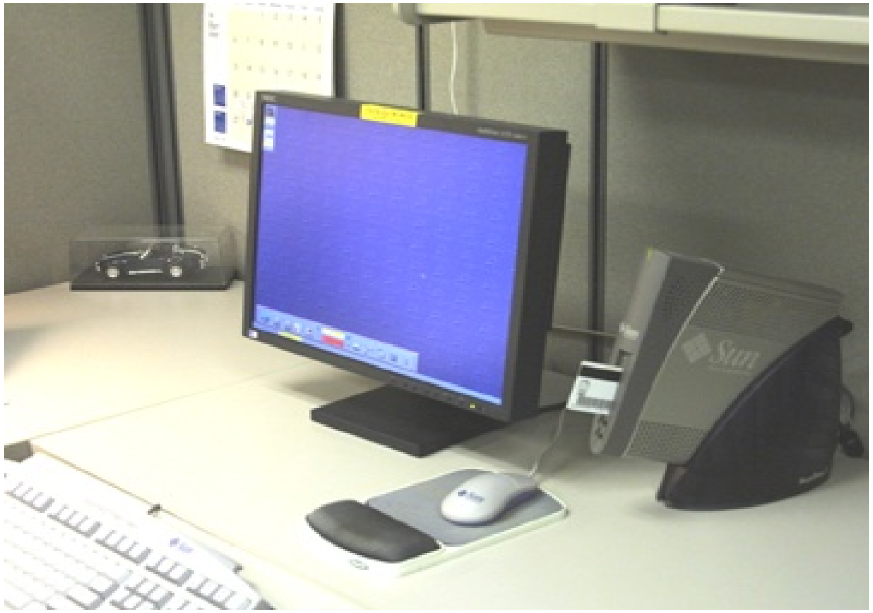
Before:

To ensure a high level of security physically isolated clients were deployed often resulting in up to 10 different PCs in a single office.

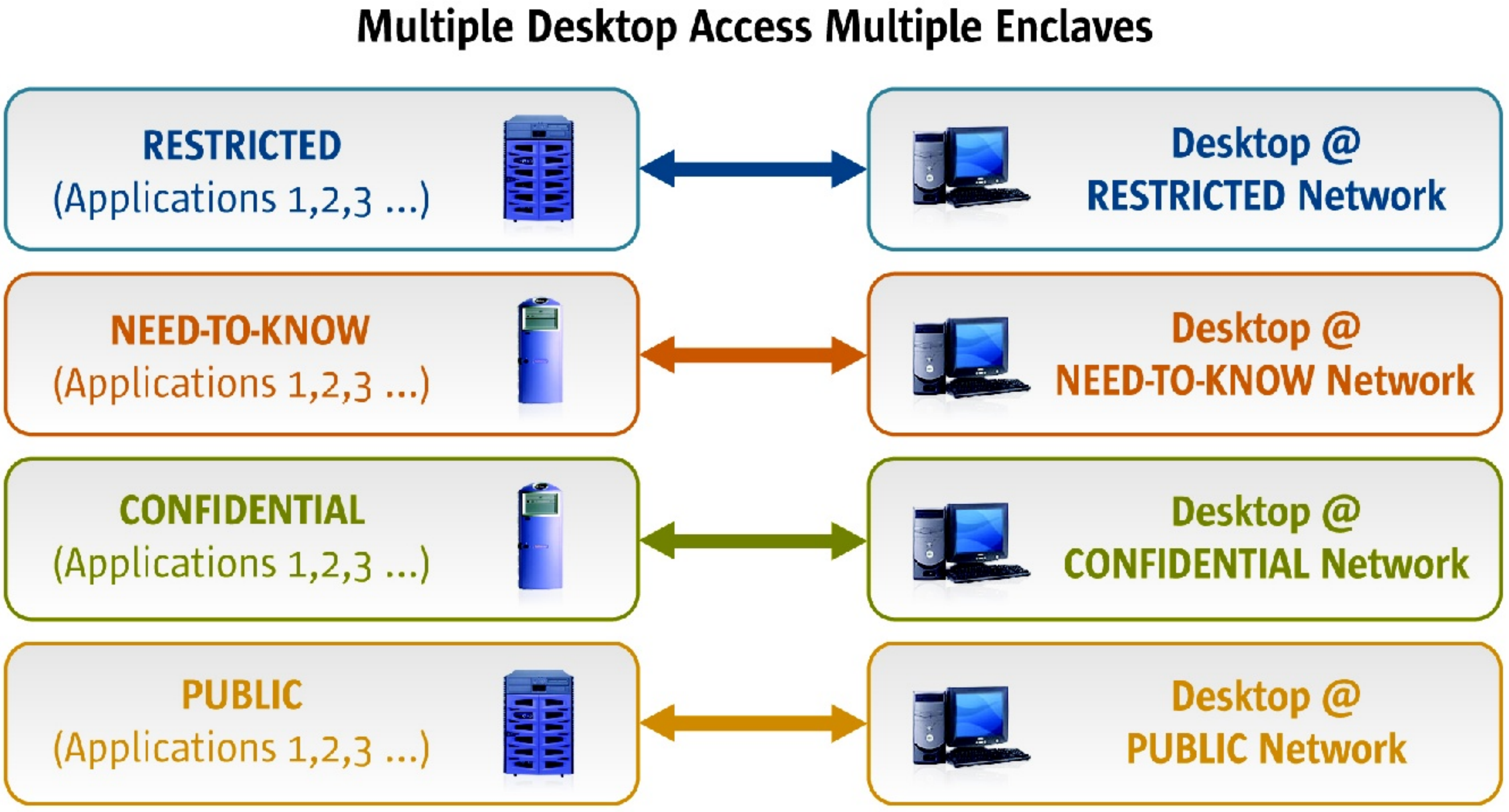


After:

Full Session Mobility enabled by a single stateless Sun Ray front-end and protected by a Trusted Solaris based back-end



Status Quo Example: Stove Piped Networks for Secure Communications



Multiple Desktop Access Multiple Enclaves

RESTRICTED
(Applications 1,2,3 ...)

Desktop @
RESTRICTED Network

NEED-TO-KNOW
(Applications 1,2,3 ...)

Desktop @
NEED-TO-KNOW Network

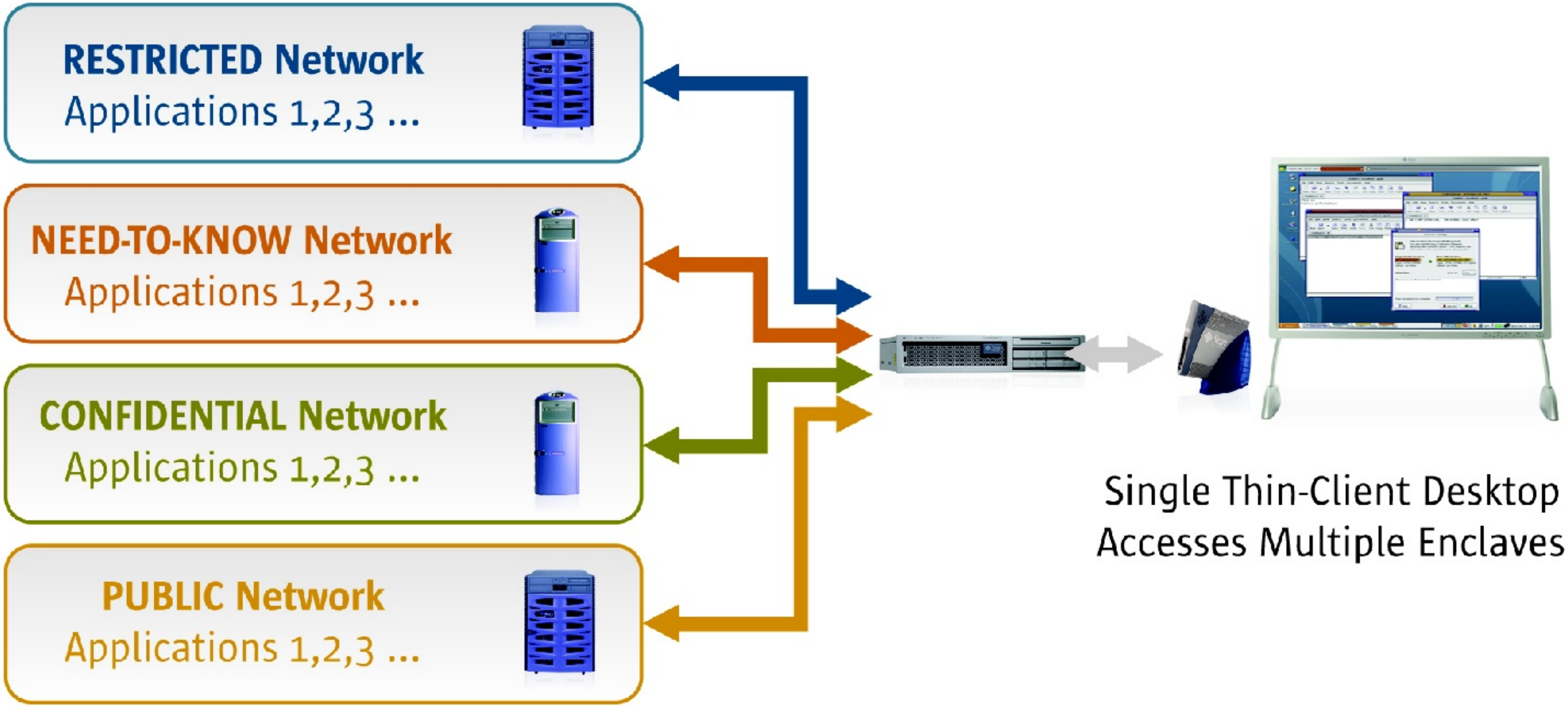
CONFIDENTIAL
(Applications 1,2,3 ...)

Desktop @
CONFIDENTIAL Network

PUBLIC
(Applications 1,2,3 ...)

Desktop @
PUBLIC Network

Changing the Game:
Single Multi-Tiered Secure Communications



RESTRICTED Network
Applications 1,2,3 ...

NEED-TO-KNOW Network
Applications 1,2,3 ...

CONFIDENTIAL Network
Applications 1,2,3 ...

PUBLIC Network
Applications 1,2,3 ...

Single Thin-Client Desktop
Accesses Multiple Enclaves

So...What's the Big Deal?

- Access ***data*** & run ***applications*** @ *multiple security levels* – from the same device. Secures and protects your data.
- 1 cable to the desktop simplify classified cable plant = **lower risk**
- Instead of maintaining 2, 3, 4, 5+ PC's @ each user's work area, you maintain ***ZERO***!
  - Greatly reducing the assets to manage, virus protect, patch.
- Lowers your overall TCO
  - Lower Acquisition costs
  - Extends System Life Cycle
  - Power, cooling, physical space
- **Accredited solution with references...**

SNAP Solution Components

- **Solaris 10 with Trusted Extensions**
- Sun Ray & Sun Ray Server Software
- Windows Interoperability (lots of options)
  - Citrix ICA
  - Remote Desktop Protocol – RDP:
    - SGD (Tarantella)
    - Sun Ray Windows Connector Client
    - RDesktop
  - VMware

MLS starts with Trusted Solaris and/or Solaris Trusted Extensions ...

- Trusted Solaris 8 HW 02/04
- Solaris Express – Nevada
- http://www.opensolaris.org
- Solaris 10 U3 HW 11/06
- Solaris 10 U4 HW 07/07

What is/are Solaris Trusted Extensions?

- A redesign of the Trusted Solaris product using a layered architecture.
- An extension of the Solaris 10 security foundation providing access control policies based on the sensitivity/label of objects
- A set of additional software packages added to a standard Solaris 10 system (hence with TX).
  - Future releases will bake TX packages in
- A set of label-aware services which implement multilevel security

Trusted Extensions in a Nutshell

- Every object has a label associated with it
  - Files, windows, printers, devices, network packets, network interfaces, processes, etc...
- Accessing or sharing data is controlled by the objects label relationship to each other
  - 'Secret' objects do not see 'Top Secret' objects
- Administrators utilize Roles for duty separation
  - Security admin, user admin, installation, etc...
- Programs/processes are granted privileges rather than full superuser access
- Strong independent certification of security

What are Label-Aware Services?

- Services which are trusted to protect multilevel information according to predefined policy
- Trusted Extensions Label-aware service include:
  - Labeled Desktops
  - Labeled Printing
  - Labeled Networking
  - Labeled Filesystems
  - Label Configuration and Translation
  - System Management Tools
  - Device Allocation

Principle of Least Privilege

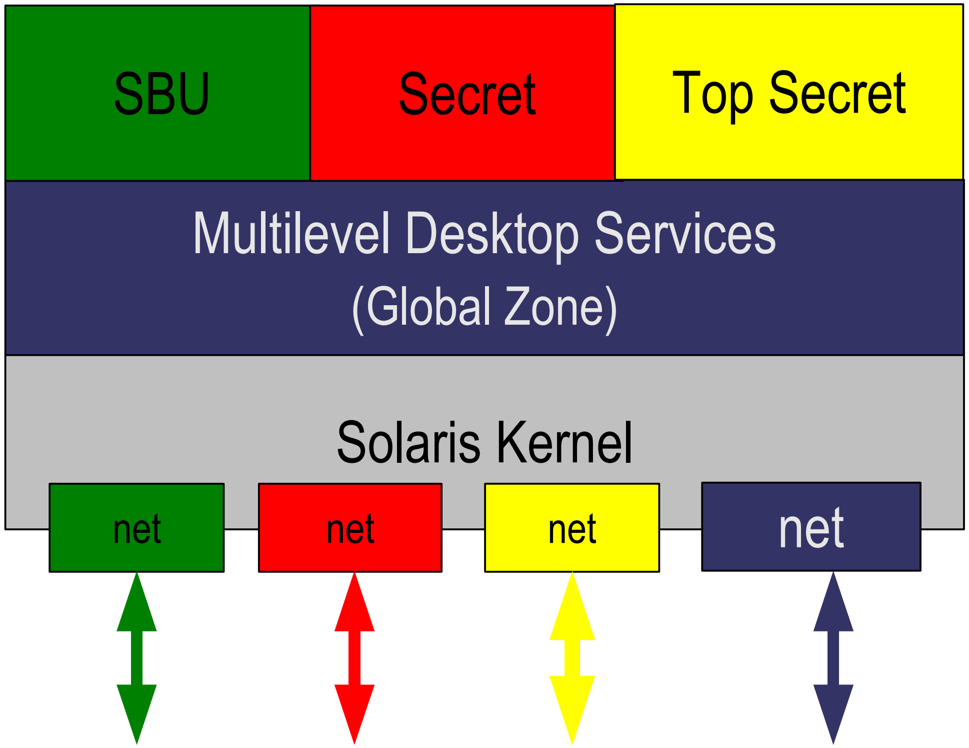
- If you don't got it, you don't get it!!!
- In traditional UNIX, root is an all-or-nothing proposition
  - > Any privileged program can compromise the whole system
- Only a small subset is usually needed
  - > Bind to reserved port
  - > Change scheduling priority
- So, we divide root's powers into discrete privileges
- Heard of SBD? No... it's not Silent But Deadly, it's
  - > Secure By Default!!!
  - > `netservices limited`
  - > 1 command & you're locked down!

Privilege Overview

- **Kernel always checks for privilege**, not uid 0
- Individual privileges can be switched on and off
  - Run with a limited subset of root's powers
  - Can make processes less privileged than normal
- Backward compatible with superuser model
- Extensible
  - Number of privileges and mapping of privilege names is private to the kernel
- Integrated with RBAC and Service Management Framework (SMF)

Multilevel Network Architecture

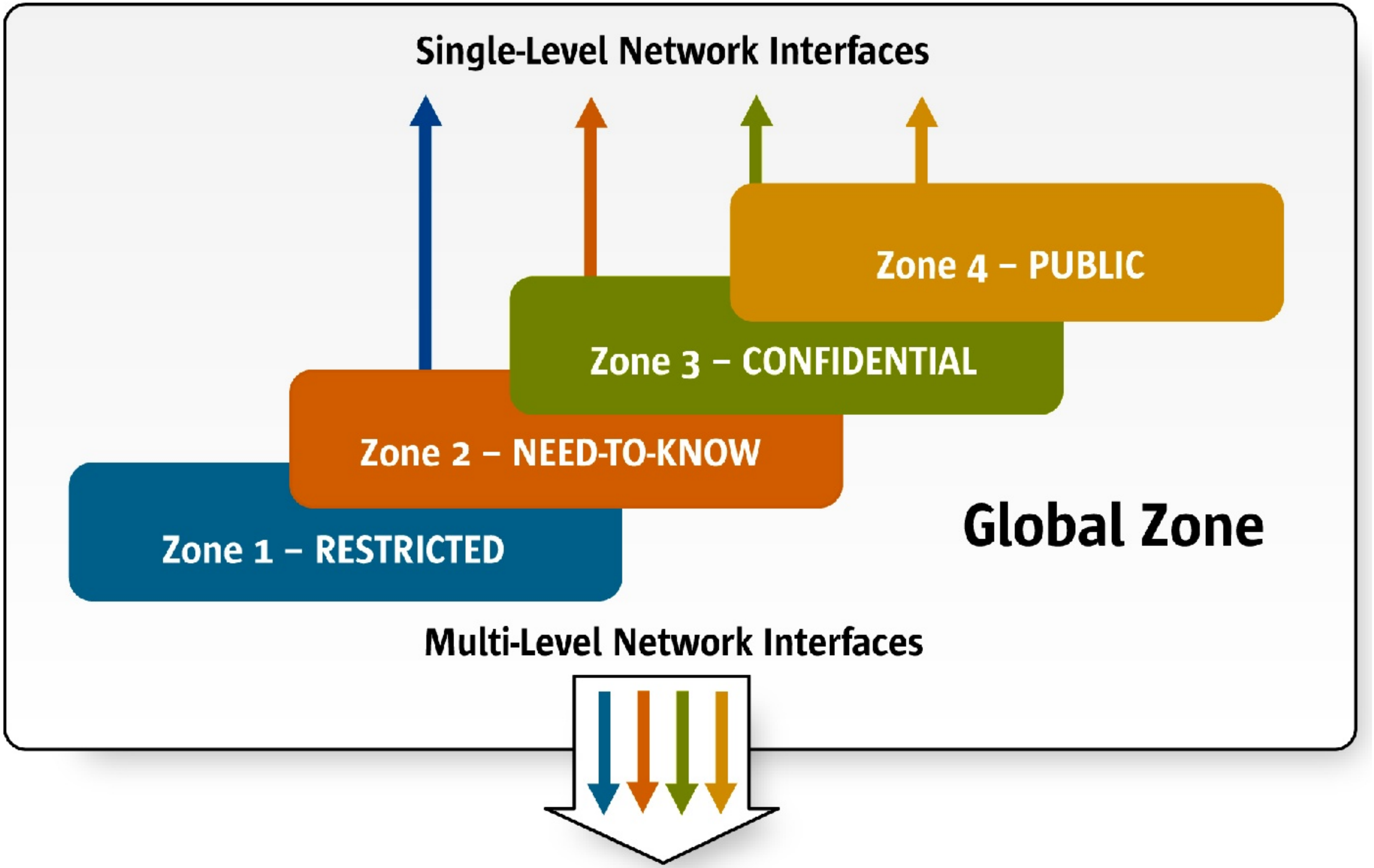
Option: 1 NIC per zone @ each security level



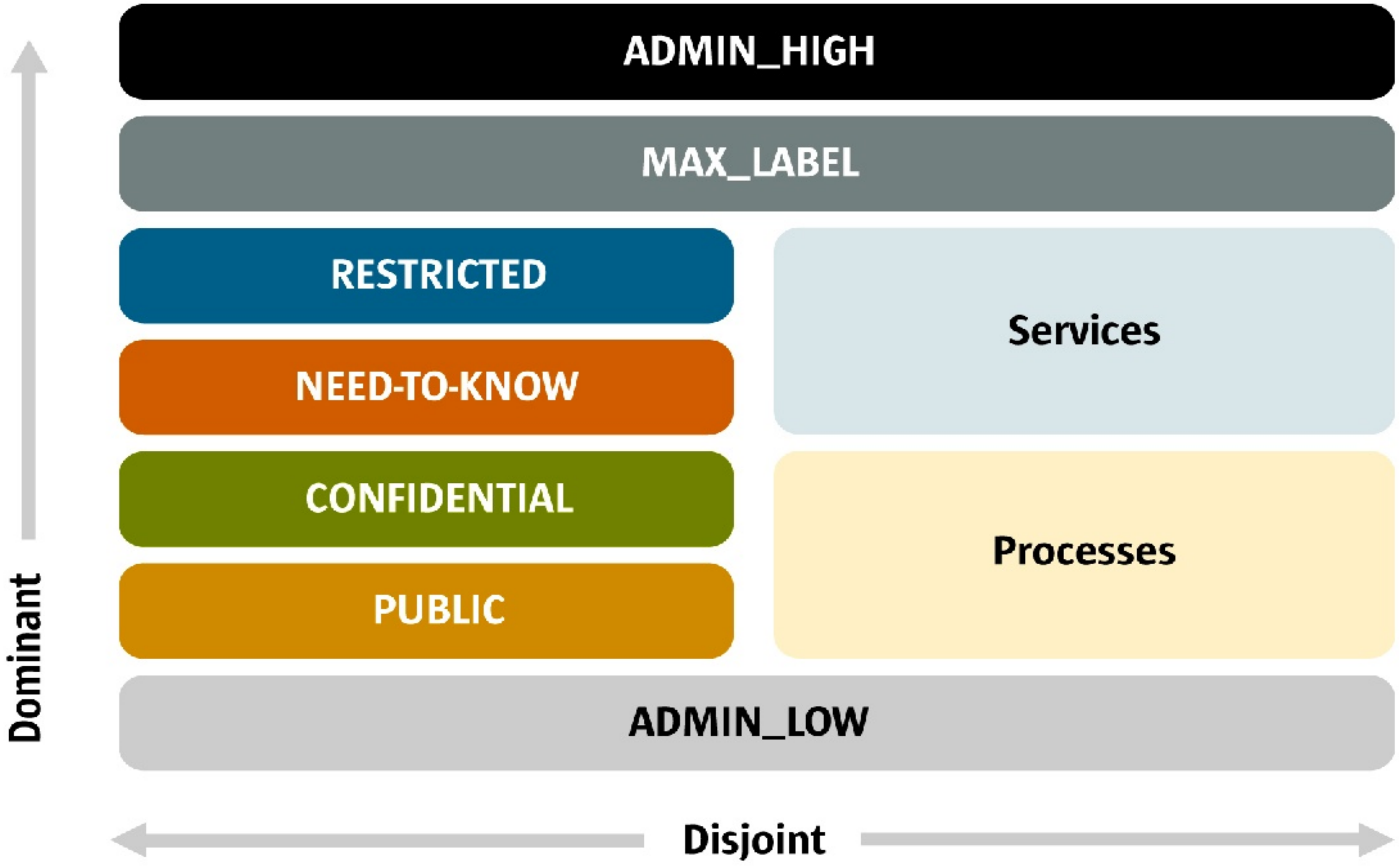
- The kernel routes network traffic to the appropriate zone based on its label and IP address
- IP addresses may be unique or shared
- Lots of options

Traditional/Accreditable: 1 NIC per label

Option: Single NIC shared by all zones



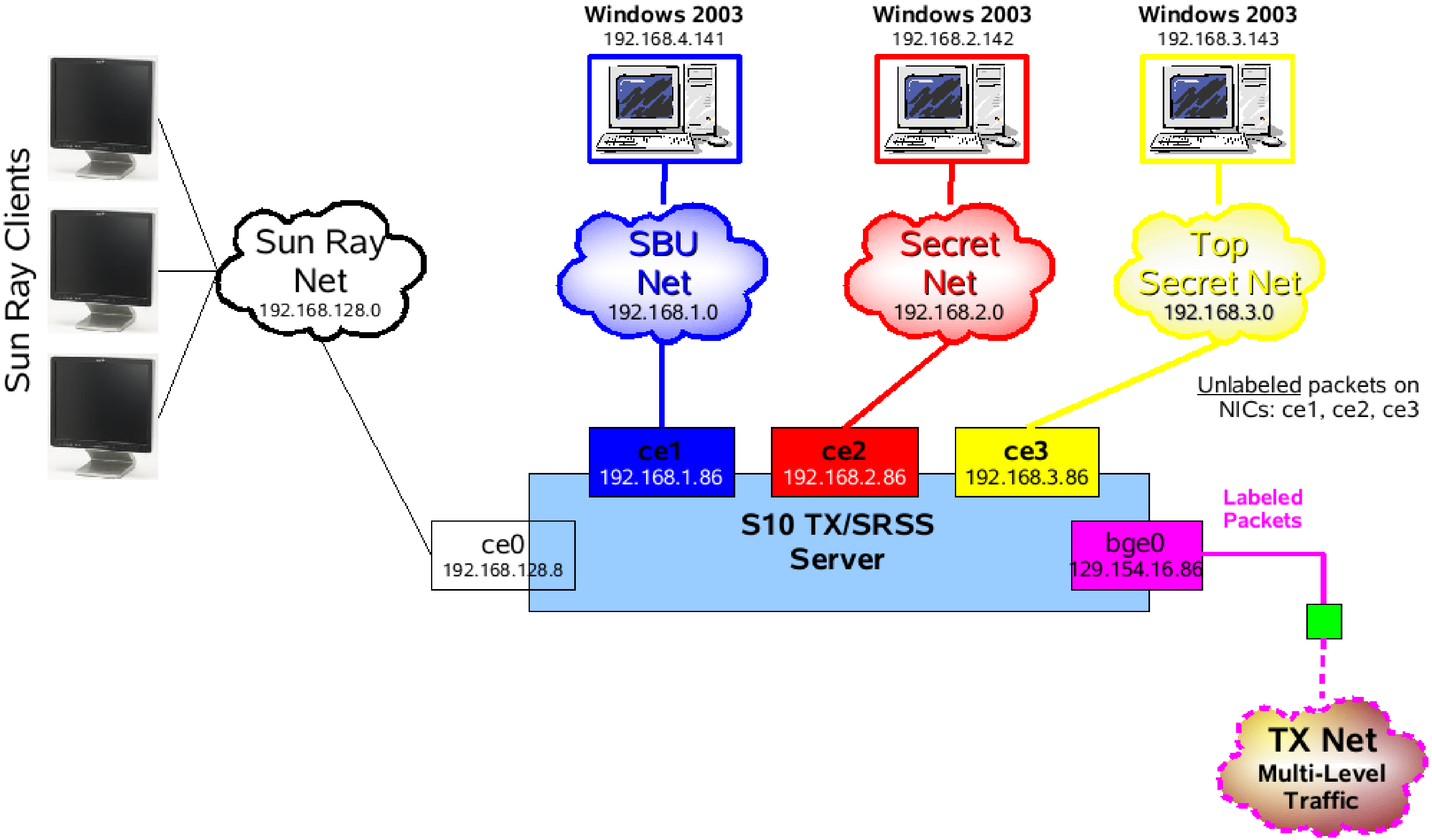
Security Label Hierarchy



Zone Concepts for Trusted Extensions

- Each zone has a label – ***Labeled Zones*** - huh?
  - **Primary function is process & data segregation**
  - Labels are implied by process zone IDs
  - Processes are isolated by label (and zone ID)
- Global zone is unique
  - Parent of all other zones
  - Exempt from all labeling policies
    - No user processes—just TCB
    - Trusted path attribute is applied implicitly
  - Provides services to other zones

Demo Configuration



Typical SRSS Install Sequence...

- utinstall; reboot
  - utadm -a *NIC* or
  - utadm -A *Subnet* or
  - utadm -L on
- utconfig
- Got that?

- It's different with SRSS on TX
  - For instance, no Kiosk Mode With TX
  - Why? Because you need a trusted window manager
  - Gotta Build A Trusted Foundation, 1st

SNAP – Foundation Work

- After Solaris 10/Reco'd Patch Cluster Install...
- Install Core Apps...
  - It's that important? Really? Yes!
  - Why? To ensure there aren't problems when you build your label zones
- Install TX Packages (in ExtraValue on DVD)
  - `java wizard`
- Define & Set site security:
  - Sensitive But Unclassified (SBU), Secret & Top Secret
  - Over simplified, but this is the foundation of TX
  - **File: label_encodings**
  - Really need to do this up front

SNAP – Foundation Work (con't)

- Setup NIC/IP definitions & Environment (2 Key Files)
  - **Security Templates: tnrhtp**
    - atohexlabel is your friend :)
  - **Database: tnrhdb**
    - Define the security level of the IP's in the system
    - How low can you go??? DTU's defined @ admin_low!!!

Build a Zone for Each Label

- zonecfg -z <zone> -f <zone config file>
- Sample zone config file for SBU Zone (TSol Template)...
  - create -t SUNWtsoldef
    - set zonepath=/zone/sbu
    - add net
      - set address=192.168.1.86/24
      - set physical=qfe1
    - end
    - commit
- ZFS is your friend, snapshot
- Install & Boot Zone
- **Speed, Simplify: Clone the other zones!!!**

Aaaaahhhh... Now SRSS

- Prequisites:
  - Install some patches & TX fixes
  - Apache Tomcat
- utinstall
  - DTU tnrhdb definitions
  - MLP's in tnzonecfg
    - Bump for X & add 7007, 7010 & 7015
    - 6000-6050/tcp;7007/tcp;7010/tcp;7015/tcp
  - Reboot
- utadm; utconfig; utrestart -c

Demos/Q&A

Thank you!

Matt Hatley
matt.hatley@sun.com