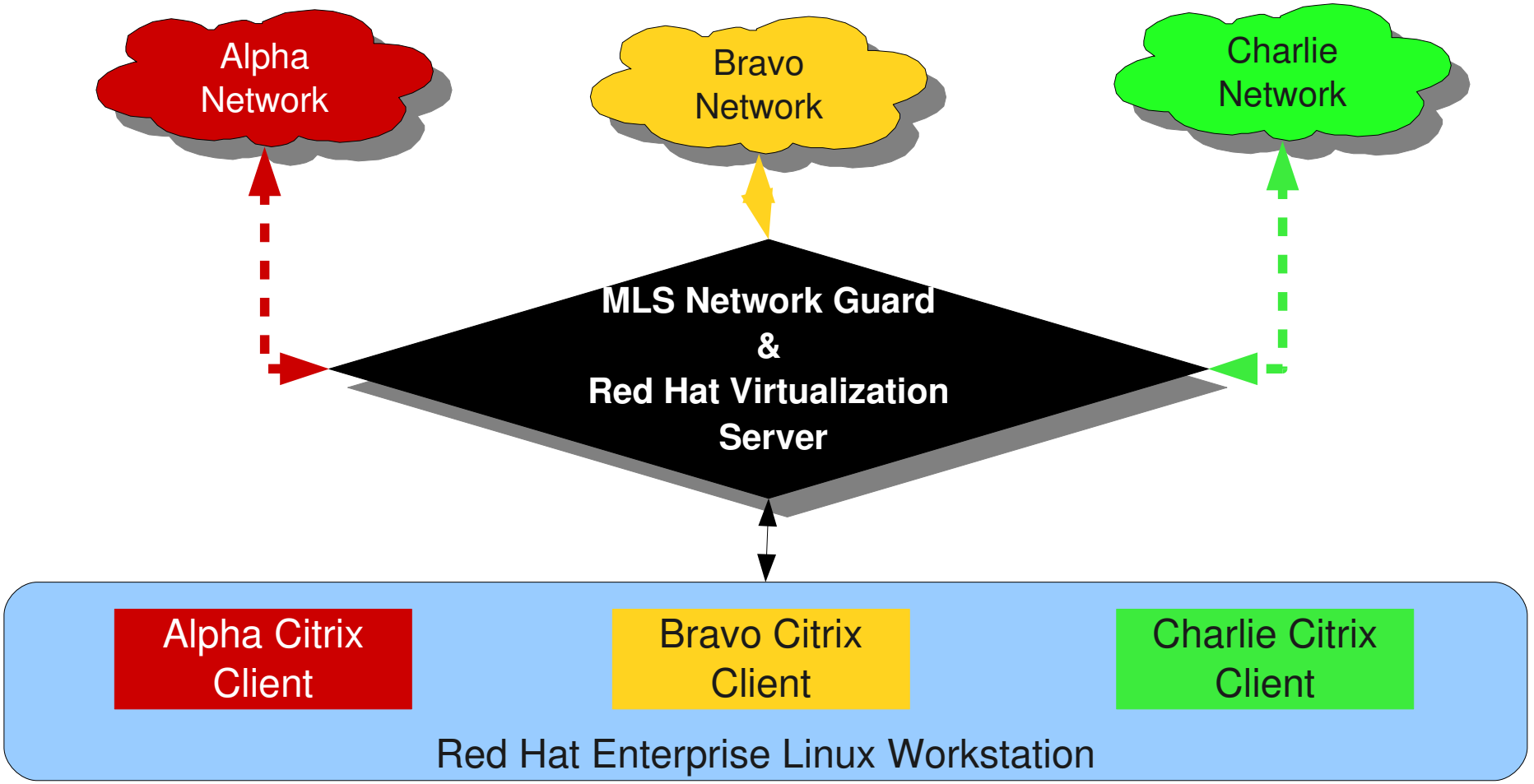
NexGen Desktop
Concept Architecture

Shawn Wells <sdw@redhat.com>
Intelligence Community Programs
443-534-0130

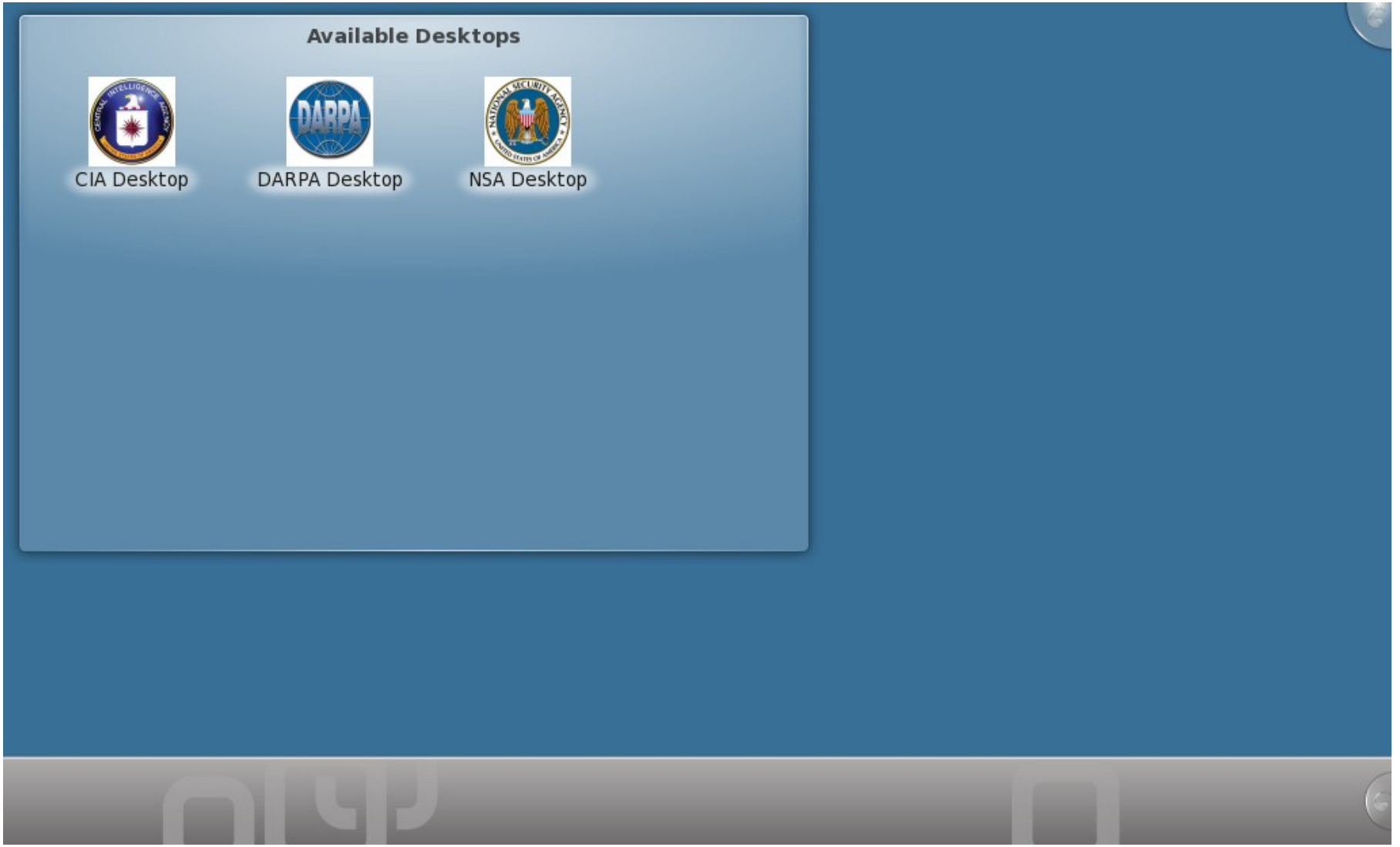
Conceptual Overview

GOAL: A light weight Red Hat Enterprise Linux based device which has the ability to have multiple concurrent Citrix sessions, each one tied to a specific network (CIA Desktop, DoDIIS Desktop, etc).



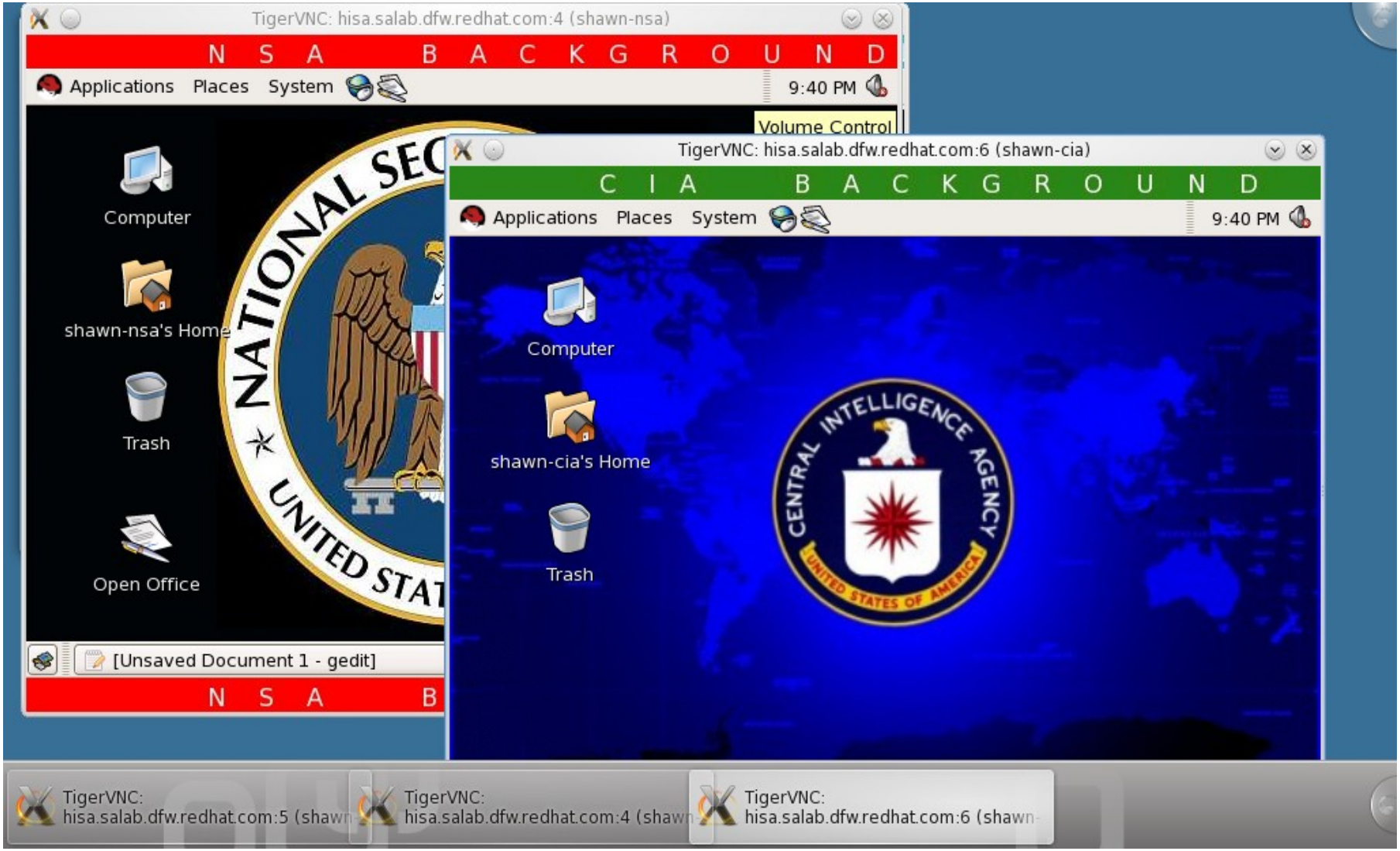
System Demonstration
&
Screen Shots

Base Desktop View



Virtual Connection View: Single Desktop

Virtual Connection View: Multi Desktop



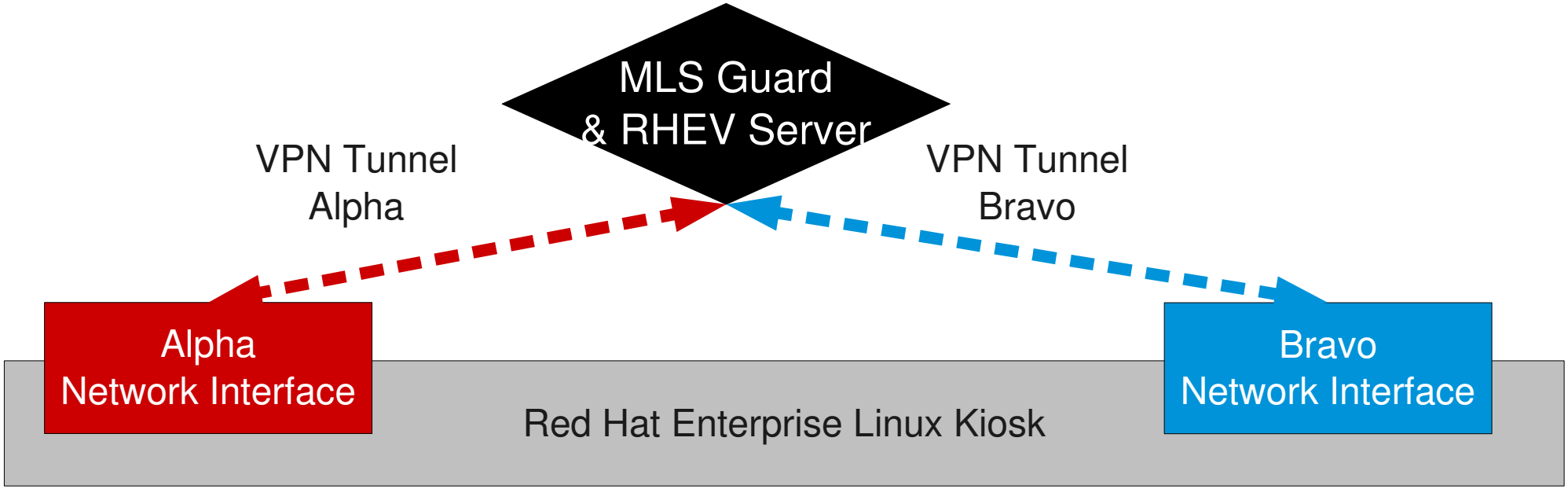
Red Hat Kiosk Security Features

Desktop System Security

- Relevant U.S. Government Red Hat Enterprise Linux 5 security certifications
  - EAL4+ Common Criteria Certification (LSPP, RBAC, CAPP) on IBM & HP hardware
  - DCID 6/3 (used up to PL5)
  - DISA STIG

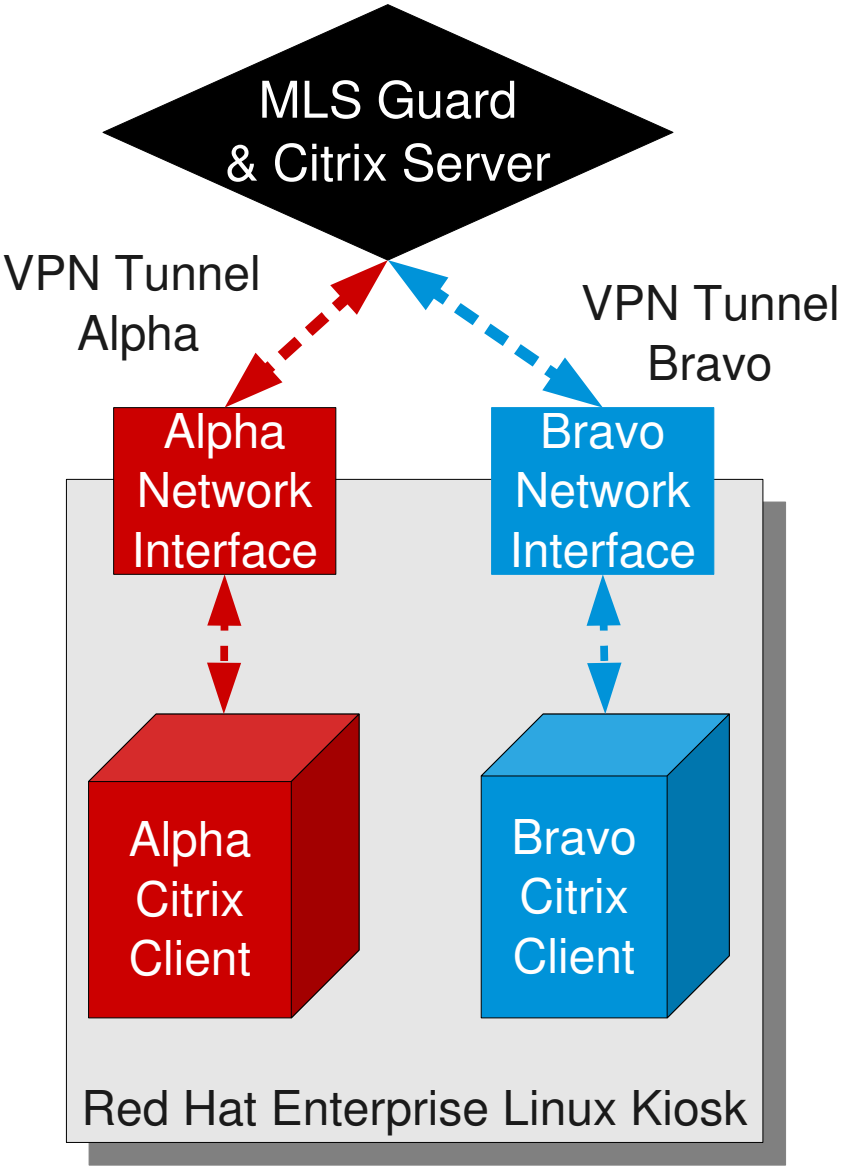
- Devices will run in “kiosk” mode
  - No ability for users to retain information or configuration locally on the system via SELinux
  - Traffic shaping technology secures network traffic to appropriate desktop/Citrix instance
  - No local users
  - No local data files
  - Inherent security, not bolt on

Desktop Firewall



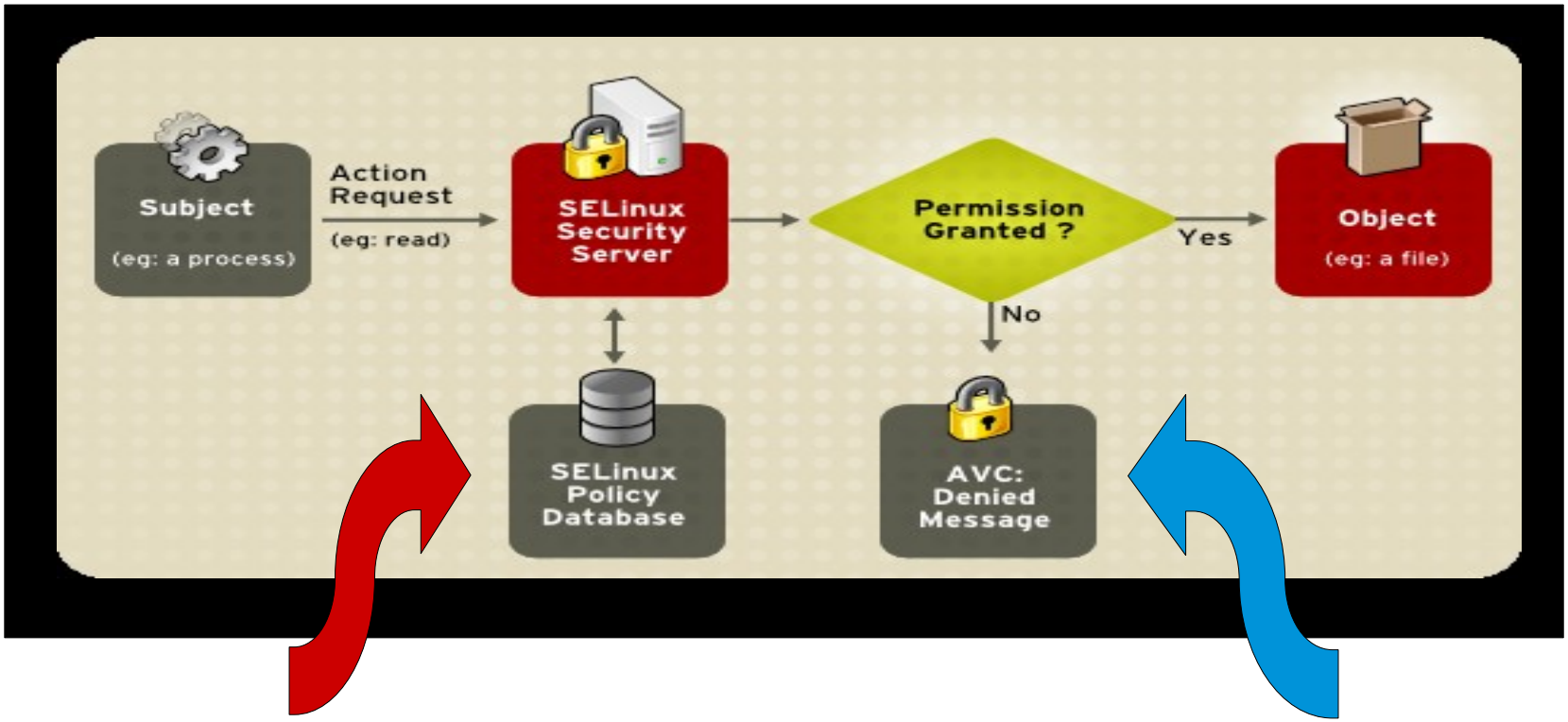
- Red Hat Enterprise Linux has embedded firewall capability, which was used in our EAL4+ Common Criteria Certification.
- Helps ensure traffic shaping should a network router become compromised.
- Policy centrally managed via Red Hat Network Satellite.

Desktop Application “Zoning”



- Utilizing a security technology named SELinux, which is co-developed with the NSA, the Red Hat Enterprise Linux Kiosk has the ability to “zone” applications and data.
  - Each network interface will be labeled, such as “Alpha Network Interface”
  - Each Citrix client will be labeled, such as “Alpha Citrix Client”
  - Security policy will check the labels, only allowing matches to establish communication paths.
- This is the same security policy used in the Red Hat Enterprise Linux Common Criteria Certification.

Short SELinux Overview



- Central management via Red Hat Satellite
- Built into system, not bolt on.
  No way to subvert access control mechanism.
- Used to audit for “covert channels” in DCID 6/3 systems

- Collected centrally on Kiosk by default
- Ability to send audit data to 3rd party applications built in
  (HP OpenView, IBM, central DB,etc)

Red Hat Kiosk
System & Software Management

Desktop System Management

- Full management by Red Hat Satellite Server, a systems management platform designed to provide complete lifecycle management of the operating system and applications.
  - Standardized Provisioning (“golden builds”)
  - Centralized software management (security patches, hardware drivers, etc)

- Same management software for both servers and desktops; one standard management suite for both

Desktop System Management: Update

Easily obtain security updates, patches, and new OS versions

Remove undesired packages through the simple RHN web interface

Automatically update systems with the latest security fixes

Desktop System Management: Manage

Manage groups of systems as easily as a single system

Assign permissions to administrators for managing different groups or roles

Schedule updates to occur during maintenance windows

Desktop System Management: Provision

Provision existing or bare metal systems using predetermined profiles or system cloning

Improve consistency by using RHN to manage and deploy configuration files

Undo problematic changes with snapshots and rollback

Desktop System Management: Monitor

Dozens of low-impact probes can be set for each system

Group probes into suites for fast deployment

Receive email or pager notices when a probe reaches a predefined warning or critical threshold

Overview

Overview

- Everything shown utilizes built in features of Enterprise Linux.
  - Built in data & network labeling technology
  - Built in auditing systems
  - Built in firewalls

- Red Hat Network (RHN) Satellite manages both existing Enterprise Linux servers in addition to desktop & Kiosk devices. Giving System Administrators the ability to manage thousands of systems as easily as one, Satellite is an integral part of the solution.