

## HP NetTop: A Technical Overview

---

### Introduction

HP NetTop transforms a single workstation into a high-assurance platform running multiple operating systems concurrently—with total domain isolation between each OS and its attached network. “Virtual Machine” (VM) vaults run operating systems such as Windows 2000, Windows XP, and Linux and execute the same office productivity and other software as standalone PCs. Users can switch between windowed VMs with a mouse click or display them full-screen one at a time. HP NetTop provides a policy-driven barrier between VMs to prevent data leakage between security domains. To system administrators and their enterprise software systems, VMs are indistinguishable from stand-alone workstations on the network. Applications like Exchange, SMS, and HP OpenView work transparently with HP NetTop VMs.

One HP NetTop workstation replaces multiple workstations in environments where data isolation cannot be compromised. In these environments, users typically access different security domains/networks from different workstations—leaving the IT organization to deal with the cost, clutter, and complexity. HP NetTop reduces the clutter and cost by leveraging advances in commercially-available virtual machine software (VMware) and operating system security (SELinux) to replace the virtual “air gap” of separate workstations traditionally used to assure domain separation.

The HP NetTop solution is based on NSA’s NetTop research project and is supported by a suite of HP services that can tailor HP NetTop to meet the needs of your unique enterprise. Assessment, pilot, rollout, and ongoing HP NetTop support at whatever level your organization requires are among the services available.

The HP NetTop solution complies with NSTISSP No. 11, and is certified by the NSA Information Assurance Directorate to provide domain separation. HP NetTop offers:

- A lower cost per seat than comparable solutions
- No special infrastructure/network architecture requirements
- No special hardware requirements—runs on a range of HP certified compatible workstations and laptops
- No hidden “gotchas”—runs standard IA32 operating systems and their applications without alteration across existing networks
- Simple installation and a small administrative footprint requiring little training and providing lower TCO

## HP NetTop: A Technical Overview

### SELinux + VMware = HP NetTop

Security Enhance Linux (SELinux) provides the foundation for HP NetTop. Briefly stated, SELinux enforces mandatory access control policies that confine user programs and system servers to the minimum amount of privilege they require to do their jobs.

When confined in this way, the ability of user programs and system daemons to cause harm when compromised (via buffer overflows or misconfiguration, for example) is reduced or eliminated. This confinement mechanism operates independently of the traditional Linux access control mechanisms. It has no concept of a “root” super user, and does not share the well-known shortcomings of the traditional Linux security mechanisms (such as a dependence on setuid/setgid binaries).

The security of an unmodified Linux system depends on the correctness of the kernel, as well as the correctness of all privileged applications and their configurations. A problem in any one of these areas can compromise the entire system. In contrast, the security of a modified system based on the SELinux kernel depends primarily on the correctness of the kernel and its security policy configuration. While problems with the correctness or configuration of applications may allow limited compromise of individual user programs and system daemons, they do not pose a threat to the security of other user programs and system daemons, or a threat to the security of the system as a whole.

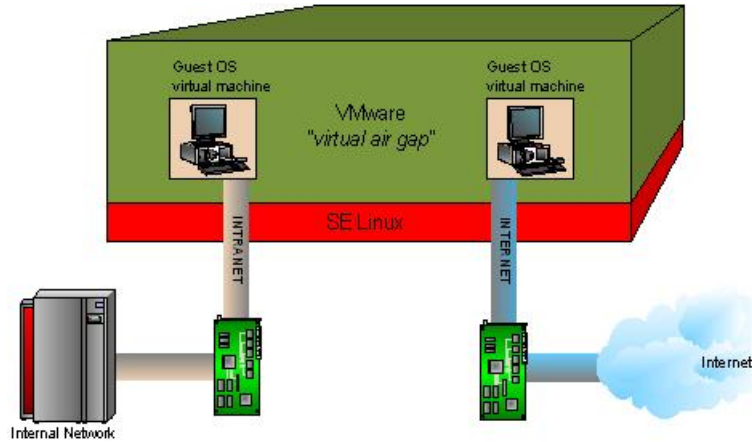
HP NetTop is a Virtual Machine Monitor application—VMware—installed on an SELinux host, with added features to guarantee system integrity during installation and use. VMware provides multiple IA32-compatible virtual machines (VMs) running on the SELinux host. Each VM can bind to its own network interface card and use VMware’s native networking capability to communicate to the network attached to the NIC—no host networking capability is required and none is installed on the SELinux host. The system disk in a VM is a set of files on the workstation disk. SELinux policy protects against data crossover between these disk files, and thus between the VMs, as the following explains.

In HP NetTop, each virtual machine is assigned a specific type (for example, `vm1_d`) and the files that contain the virtual disks are assigned a different type (for example, `vm1_t`). Each virtual machine type `vmX_d` (where X is an arbitrary number) can only access files (virtual disks) of type `vmX_t`. In HP NetTop, the SELinux policy is written such that only VMs can access virtual disk files, and a VM can only access its associated virtual disk. No other process (including other VM's) has permission to access a VM's virtual disk. This includes processes that execute with root permission.

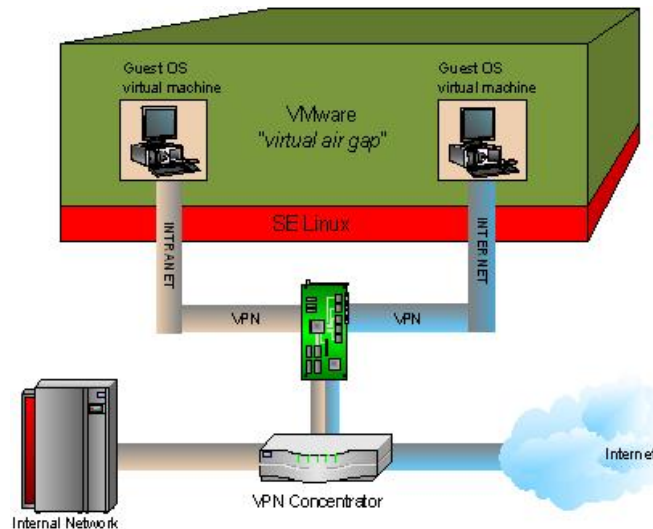
In systems where data separation is important, being able to show that data cannot flow between networks (or in this case from one VM to another) is an important property of a mandatory policy. In the HP NetTop policy, the VMware virtual machines are isolated from the rest of the system. Data flows into and out of a virtual machine only if the policy allows it. SELinux also provides an extremely robust access violation logging facility that logs policy violations attempted by any process or entity. With its native log retrieval mechanism, HP NetTop provides ISSOs a mechanism for continuous oversight of HP NetTop workstations, and since the daemons and applications that normally provide network connectivity have been removed from the HP NetTop host, ISSOs can be assured that the only data entering and leaving an HP NetTop system is through the VMs—never the host.

## HP NetTop: A Technical Overview

Between the VM vaults provided by SELinux policy and the absence of any communication interface in the HP NetTop SELinux host OS, HP NetTop can be viewed as a software KVM device for switching between VMs. A default HP NetTop configuration of two VMs is pictured below.



You don't need separate networks and multi-NIC workstations to benefit from HP NetTop. HP NetTop works with VPNs to provide end-to-end data encryption between different VMs and their VPN termination points. In the same way that VMs can be bound to different physical NICs connected to different network backbones, this single network solution allows HP NetTop to be used in any network where secure data separation is required.



### HP NetTop Applications

HP NetTop solutions are installed in major intelligence and defense facilities worldwide. However, HP NetTop solutions can be used anywhere data isolation must be maintained. Some examples are:

#### Help Desk

Many organizations outsource help desk operations to IT service providers. The help desks may be located at the customer site or at a centralized site maintained by the service provider. Help desk agents need access to all of the customer's network to diagnose problems, collect log files, etc. At the same time, they need access to their own internal network to tap knowledge bases, download patches, use trouble ticket systems, and access company email. As a result, agents often require two PCs with a single keyboard, mouse and monitor on a KVM switch.

NetTop reduces the hardware to a single PC with one or more NIC cards, and provides the additional advantage that help desk agents can have two windows open simultaneously on one display, one providing access to the problem system on the customer network, and the other displaying a knowledge base article about the problem. The VM attached to the customer network would typically be loaded with a customer's standard software, incorporating any necessary additional software products and authentication software.

This scenario can easily be expanded to a case where the service provider remotely manages the customer's servers and network equipment. A third NIC could be added to the HP NetTop system and a minimal Linux OS loaded in a third VM to provide Secure Shell (SSH) access to the customer's private network infrastructure systems (routers, switches, SAN, etc) or to Unix servers. Currently, there are HP NetTop systems deployed that support seven simultaneous network connections using multi-port NIC cards.

#### Government Agency

Many agencies have multiple limited-access networks which contain sensitive data. Examples are connections to law-enforcement networks and internal networks used by the Office of Inspector General or finance department. Personnel working in these agencies also need to access the agency Intranet for email, time and attendance information, internal web servers with project and benefits information, etc. There might be legacy applications that are only supported under an older operating system, for example, a proprietary database in the finance department that only runs under Windows NT, while the rest of the agency runs Windows XP. HP NetTop provides a single PC that can support these different networks and operating systems in a secure manner, permitting no data to pass between them.

#### Defense Contactor

Defense contractor software engineers often work on-site at DoD facilities and frequently work on multiple projects, where each project is housed in a closed lab with its own private network. These engineers need access to the lab's private network as well as access to their corporate Intranet (and Internet via proxy) for email, time card entry, periodic reporting, Instant Messaging, and so on. HP NetTop can provide a single PC running Windows XP in one VM for the corporate Intranet and Linux in a second VM for Java development and access to project X, and Windows 2000 in a third VM for project Z.

### Wall Street Financial Firm

The section of a large firm that handles mergers and acquisitions has a separate network of servers and workstations to protect this highly sensitive information, as required by law. The employees in this section also need to access databases on the corporate network and to send/receive email. An HP NetTop system provides access to both networks in a secure, independent manner.

### HP Service Leadership

HP NetTop is backed by HP's:

- Highly trained consultants and technical specialists with industry-recognized security certifications
- Worldwide security solutions delivery and support
- In-depth expertise across today's security landscape, including technologies for firewalls, VPNs, authentication, identity management, and access control.

HP recognizes your enterprise may have unique security requirements that require a customized solution. Therefore, the HP NetTop solution is offered as an integrated system of software and services that tailor HP NetTop to your specific environment. HP offers a menu of services to assess customer environments, tailor a security policy solution, pilot and roll out the solution, and provide documentation, administrator training, and continued software upgrades and support.

### For More Information

Contact the HP NetTop team at:

phone: 1-888-302-7339

email: [nettop@hp.com](mailto:nettop@hp.com)