Carnegie Mellon University
Software Engineering Institute

vTunnel

Hide Administrative Traffic from Exercise Participants

DELIVERING EFFECTIVE HANDS-ON TRAINING REQUIRES THE CREATION OF COMPLEX ENVIRONMENTS THAT LOOK LIKE THE REAL WORLD. But how realistic can training be when administrative (i.e., background) traffic is visible in the exercise? You can't expect exercise participants to simply ignore administrative traffic, and seeing it can compromise the realism and objectives of training. Also, when operators secure the network, they run the risk of blocking administrative traffic and breaking the exercise.

Hiding Administrative Traffic

At the Software Engineering Institute, we developed a tool called vTunnel to hide network traffic that you don't want cyber-event participants to see. As shown in the figure below, vTunnel allows IP traffic to be tunneled from a guest virtual machine through the hypervisor communication interface (the same interface used for VMware Tools). This tunneling enables administrative traffic to be removed from exercise networks, completely hiding the traffic from participants.

Implementation Options

vTunnel has multiple implementation options, including combinations of different hosts that work with several guests, such as ESXi, Windows, or Linux hosts working with different combinations of Windows, Linux, VMware Workstations, and QEMU guests.

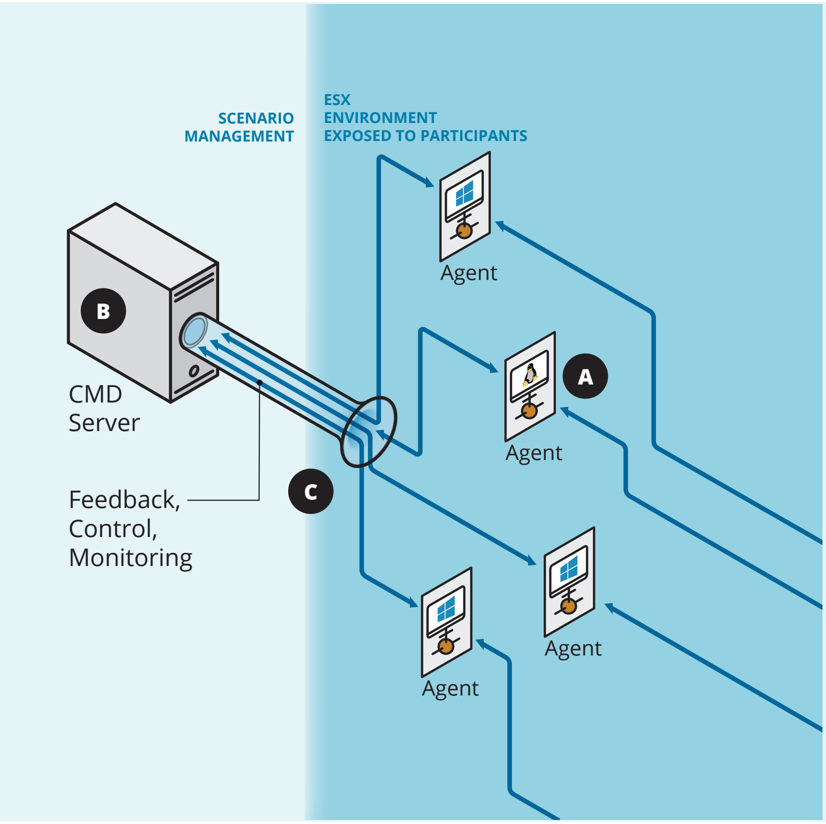
What Does vTunnel Hide?

Cybersecurity training often involves two important administrative functions: monitoring and scoring exercises, and performing command and control activities. vTunnel hides the traffic generated by these two key functions.

- For scoring exercises, vTunnel daemons are configured to allow connections into the guest virtual machines. For example, log entry data from Syslog messages can be sent from the guest machine to a log aggregation system, such as Logstash, running in the ESXi host's network. The client and server programs, Syslog and Logstash, have a tunnel vTunnel connection established between them, and they can behave as if they are directly connected with IP.

- For command and control, vTunnel enables command traffic to GHOSTS, a non-player character orchestration generator that creates realistic character actions and reactions. By communicating with a GHOSTS client on the guest system, that client can emulate user activities on the system. When utilizing vTunnel to connect these systems, the command and control traffic is hidden from the users.

You can also apply vTunnel to other uses, such as configuring systems with ansible via winrm/ssh, logging student activity on guest systems to a central location, and more. Since vTunnel works with any IP-based application, there is unlimited potential for its use by mechanisms that support cybersecurity training. Therefore, vTunnel allows greater control of your cybersecurity exercises and enables you to provide more effective training.


SCENARIO MANAGEMENT
ESX ENVIRONMENT EXPOSED TO PARTICIPANTS
B
CMD Server
Feedback, Control, Monitoring
C
A
Agent
Agent
Agent
Agent

vTunnel Highlights

vTunnel offers the solution for keeping management and control traffic out of the game space.

A. vTunnel creates non-Ethernet connections through the VMware hypervisor as an alternate path for passing management and monitoring data flows.

B. Command and control traffic is also delivered via vTunnel, including traffic to GHOSTS NPC users performing operations on systems in the environment.

C. vTunnel supports data gathering for monitoring and aggregation at a collection server, as well as for automated scoring of cyber-training events.

Explore Our Tools Online

SEI cyber training tools can be used to create cybersecurity training to help students learn in near-real-world situations without risking organizational assets.

See the latest information about these tools on our website at **sei.cmu.edu/go/cwd-tools**.

About the SEI

The Software Engineering Institute is a federally funded research and development center (FFRDC) that works with defense and government organizations, industry, and academia to advance the state of the art in software engineering and cybersecurity to benefit the public interest. Part of Carnegie Mellon University, the SEI is a national resource in pioneering emerging technologies, cybersecurity, software acquisition, and software lifecycle assurance.

Contact Us

CARNEGIE MELLON UNIVERSITY
SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE; PITTSBURGH, PA 15213-2612

sei.cmu.edu
412.268.5800 | 888.201.4479
info@sei.cmu.edu