



Host-based Firewall With Dynamic Encryption Capability

Kurt Sherman

ksherman@mitre.org

Deborah Tran

dtran@mitre.org

CEM IR&D

Problems

- **Judges' e-mail and other network traffic may contain sensitive or restricted data**
- **Each local network is independently managed, complicating central attempts to deploy security measures**
- **Judges' privacy concerns conflict with network management models due to deep packet inspection capability**
- **Efforts to install converged services such as VoIP and VTC are hindered due to a lack of end-to-end network management capability**

Background

- **Sponsor network does not include secure or encrypted support for classified data**
- **Data traverses both local and carrier infrastructure in the clear**
- **Judicial concerns focus on ability for central management monitoring to track usage patterns**
- **Threat of eavesdropping or “man-in-the-middle” attacks, although slight, does exist**

Objectives

- **Year 1**
 - **Develop user transparent dynamic encryption model**
 - **Deploy proof-of-concept on Linux platform**
 - **Present to peers to vet concept and approach**
- **Year 2**
 - **Migrate to Windows platform**
 - **Determine performance impact**
 - **Prepare technology transfer to sponsor**

Activities

■ Year 1

- **Develop host-to-host transport VPN using open source software and host-based firewalls**
- **Session in place only while needed (dynamic)**
- **Central policy server used to push rule sets to desktops**
- **Completely transparent to the end user**
- **Linux prototype developed**

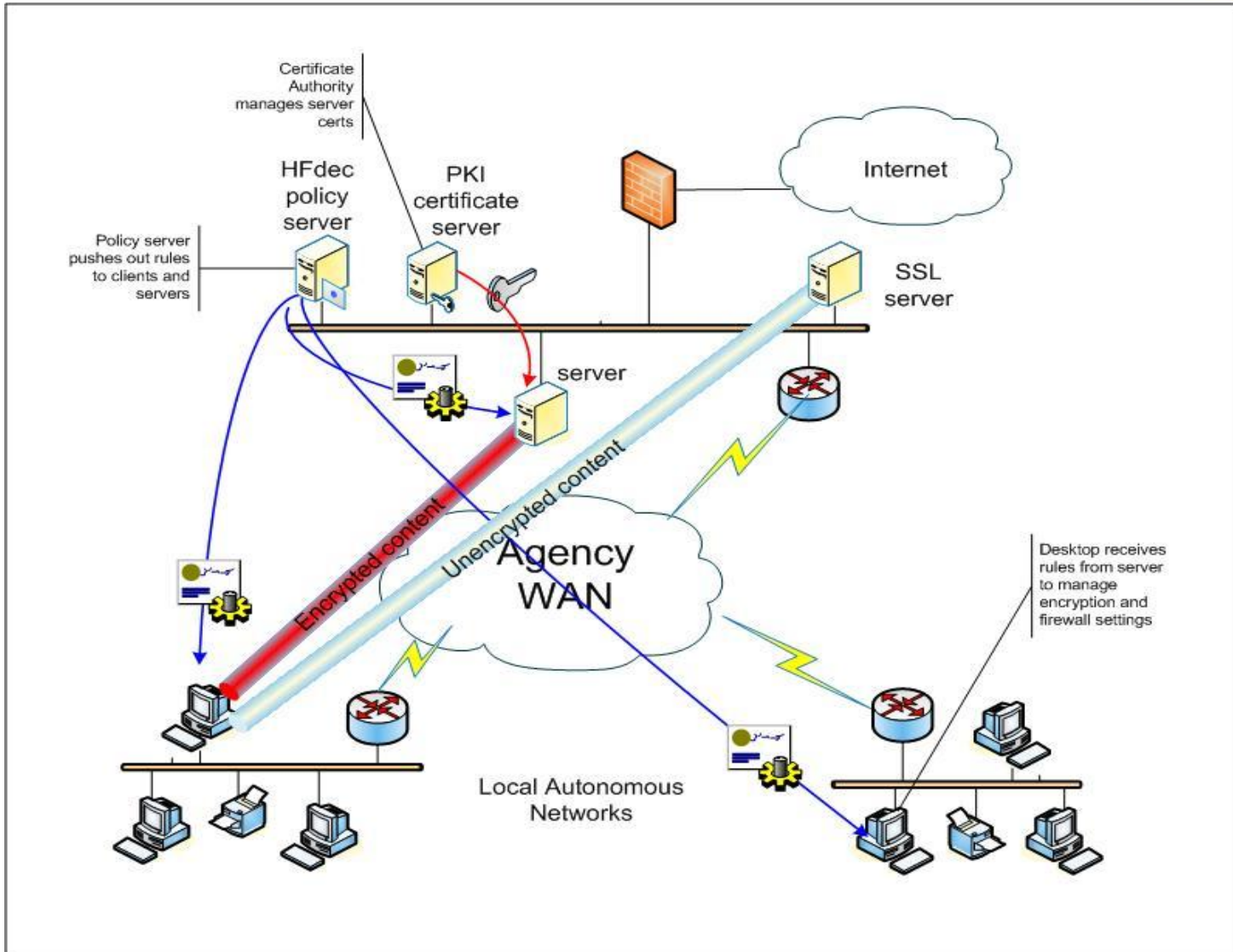
■ Year 2

- **Migrate functionality to Windows platform**
- **Perform performance testing**
- **Enhance policy server**
- **Determine standards compliancy (i.e., OpenSSL implementation in OpenVPN)**

Highlights

- **Model provides secure end-to-end communications transparent to user**
- **OpenVPN provides lightweight, robust alternative to configuration-intensive IPSec implementations**
- **Mesh capability supports multiple concurrent secure sessions**
- **Provides ultimate layer to “defense in depth” model**
- **Policy server dynamically updates clients with new server resources**

Demonstration



Impacts

- **Eliminates insider threat**
- **Addresses privacy concerns by encrypting packet payload**
- **Applicable to other agencies sharing network infrastructure**
- **Portable to internet-based deployments (i.e., perimeterless networks)**
- **Does not rely on added hardware for functionality**

Future Plans

- **Address outstanding objectives**
 - Performance testing
 - Implement PKI option
- **Beta test at sponsor location**
- **Optimize code**