Virtual Private Networking

KSU IT Security Training
April 13, 2011
Presenter : Audrey Hubbell
The State of VPN @ K-State

Hardware:

• Cisco 3000 VPN Concentrator

• ASA 5550 VPN Failover Pair
The State of VPN @ K-State

IPSec VPN:
• Majority of users connect through IPSec
• Client administration is mostly manual
• Not all external network environments are “IPSec-friendly”
• Passkeys are easily decoded
• Until recently, Cisco had no 64-bit client
The State of VPN @ K-State

SSL VPN - Any Connect:
• Client Administration is automated
• Support for Windows 32 and 64-bit, MacOSX Intel and PowerPC, Linux, and Mobile Devices
• Universal Use via HTTPS
• Authentication restricts un-authorized use
The State of VPN @ K-State

SSL VPN - Any Connect (continued):
• Designed for latency-sensitive traffic (DTLS)
• Functions in extreme latency/low bandwidth circumstances
• Beta Test
The Road Map

Goals:

• Transition all profile groups off of the Concentrator

• Move from IPSec to SSL VPN
Road Map

Phase 1

• Offer Any Connect general VPN services to all Faculty and Staff

• Start trial for Any Connect services April 18, 2011
  Parking, DARS, Lafene, & CDC
Road Map

Phase 2
• Cutover to SSL only VPN for the transition groups in Phase 1 (target May 3, 2011)

Phase 3
• Cutover groups from the Concentrator
“How To” Any Connect

- Download the client via http://www.k-state.edu/its/security/vpn/

- IPSec client and Any Connect client can co-exist
“How To” Any Connect
“How To” Any Connect
“How To” Any Connect
Why SSL VPN?

- Easily administered, scalable
- Less chance for un-authorized use
- Universal Use via HTTPS
- Stable in high latency/low bandwidth
- A secure way for K-Staters to stay connected