

Virtual Private Network Enhancements Since Windows Server 2003

Joe Davies

Principal Writer

Windows Server Documentation

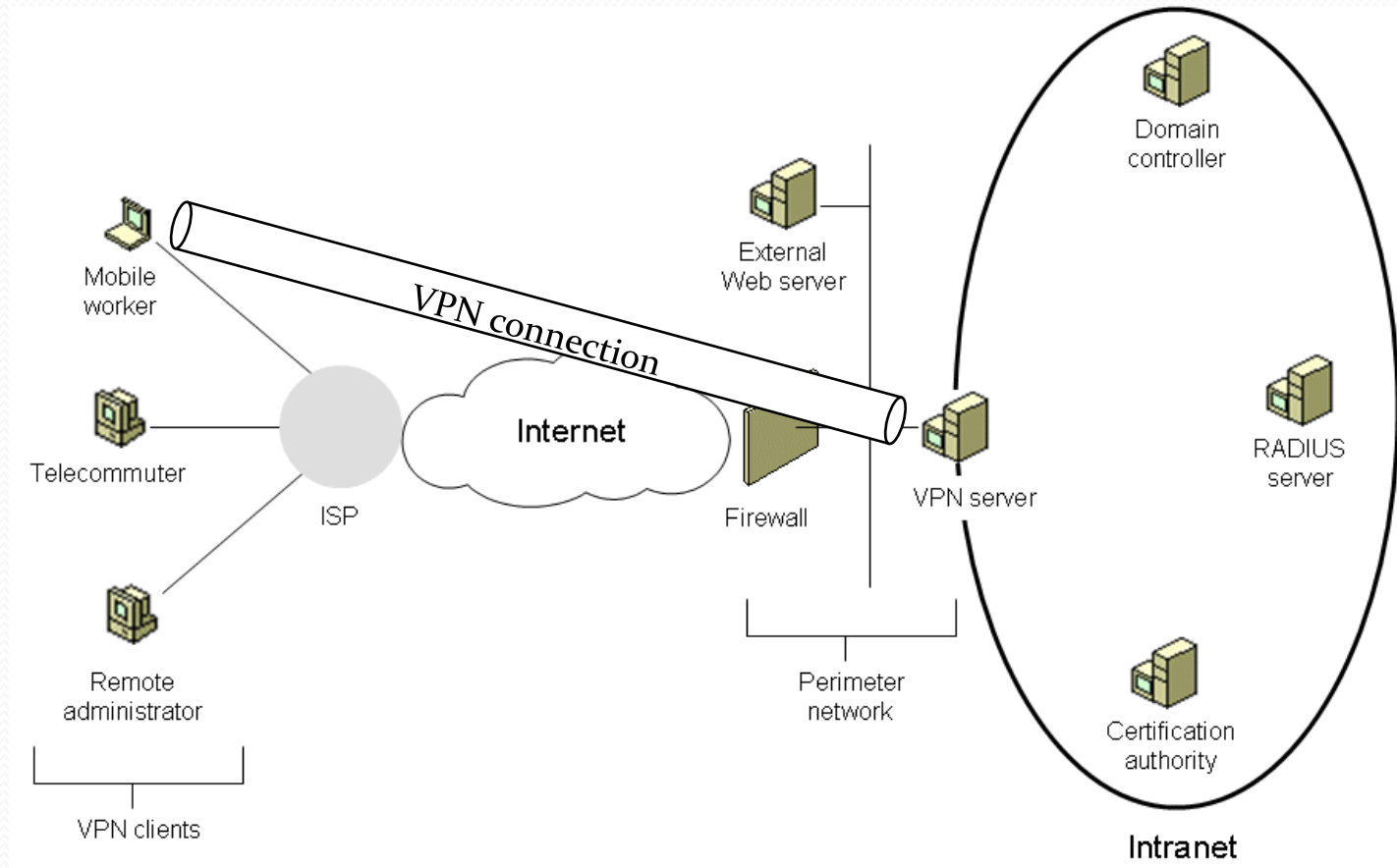
Presented at *Seattle* Windows Networking User Group monthly meeting
September 1, 2010

Agenda

- Brief VPN technology overview
- VPN features in Windows Server 2003/Windows XP
- VPN features in Windows Server 2008/Windows Vista
- VPN features in Windows Server 2008 R2/Windows 7

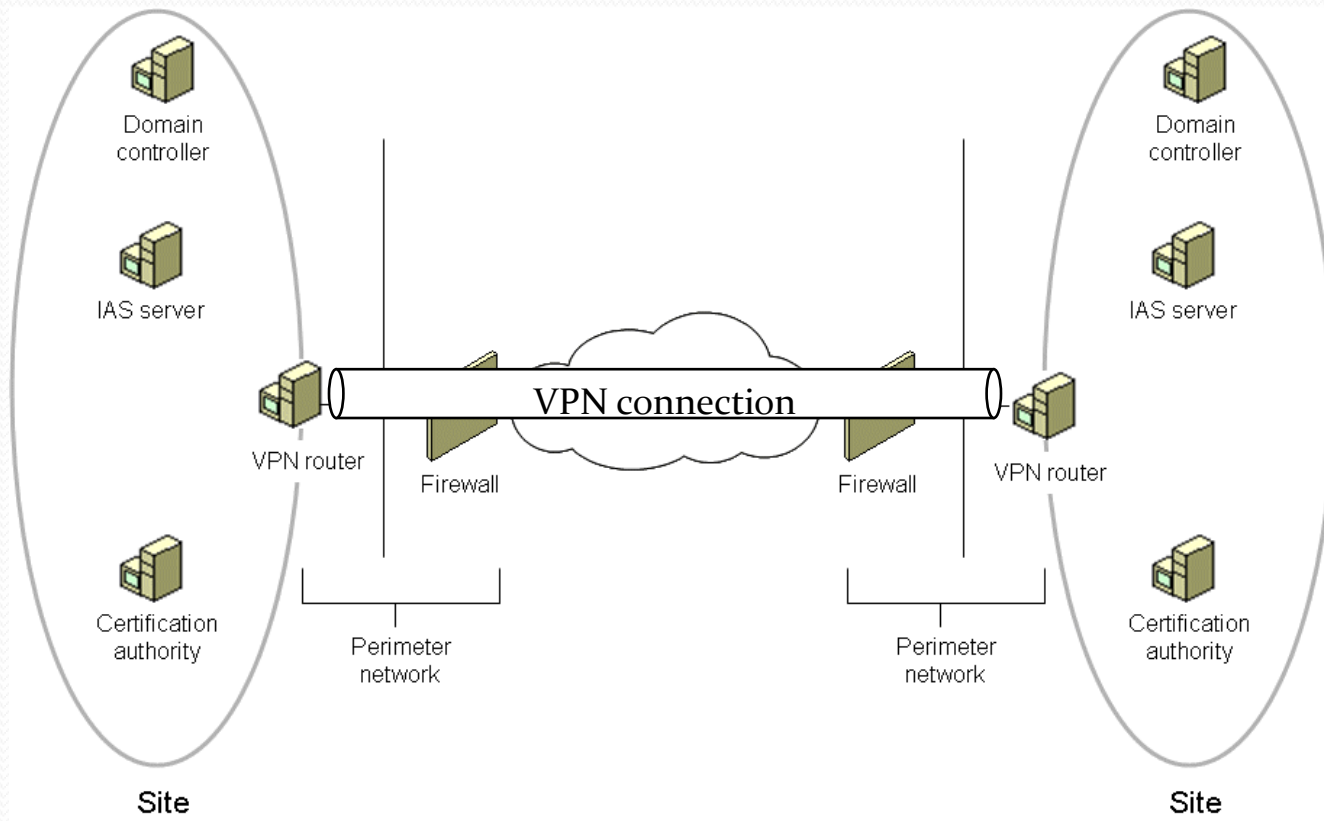
VPN technology overview

- Remote access VPN



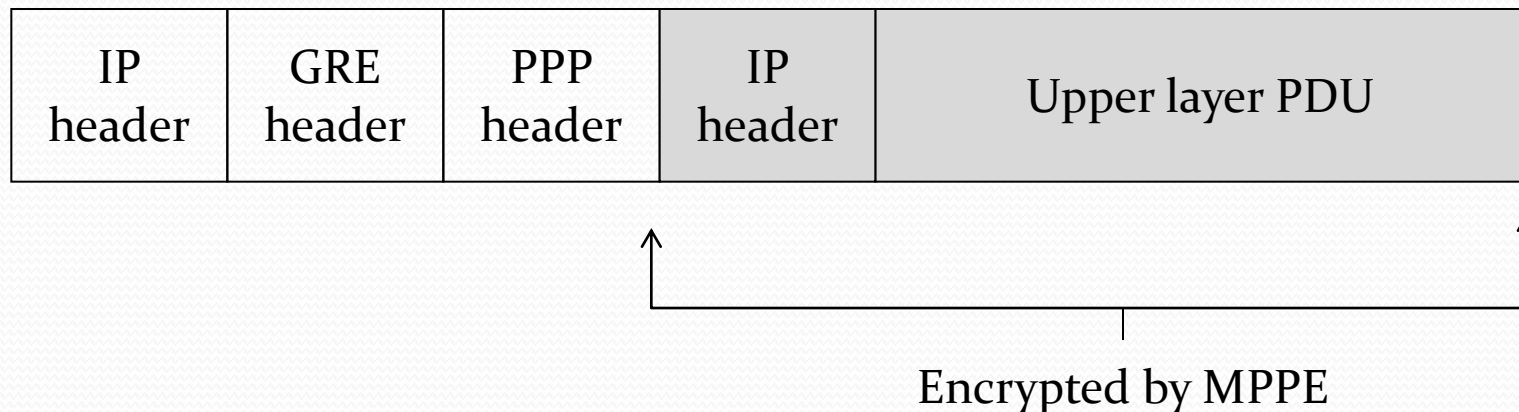
VPN technology overview

- Site-to-site VPN



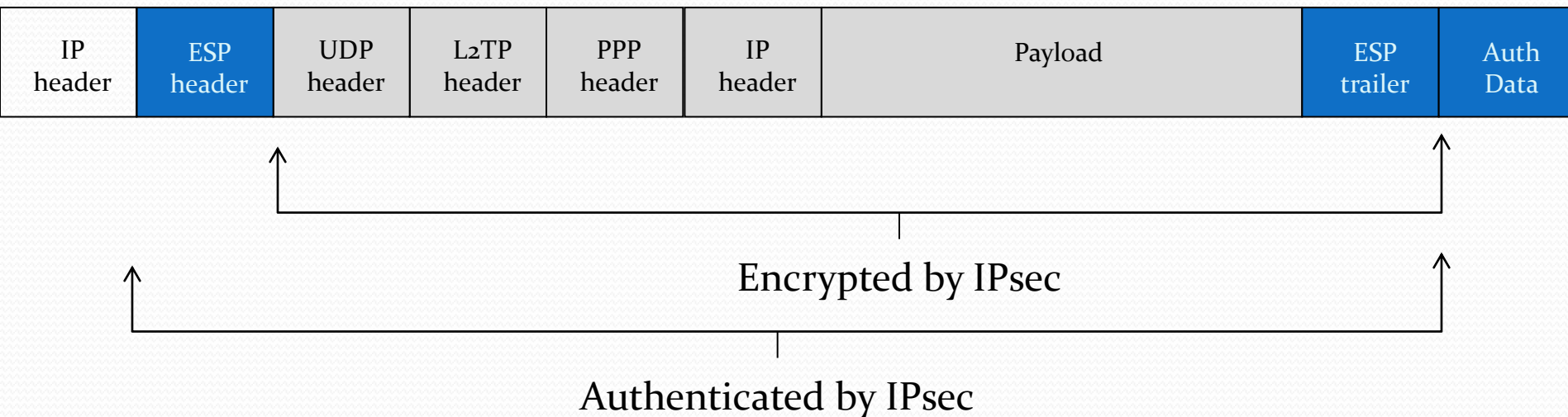
VPN technologies in Windows Server 2003/Windows XP

- VPN protocols
 - Point-to-Point Tunneling Protocol (PPTP)
 - Password-based authentication possible
 - 128-bit Microsoft Point-to-Point Encryption (MPPE)



VPN technologies in Windows Server 2003/Windows XP (cont.)

- VPN protocols
 - Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)
 - Certificate-based authentication
 - Transport mode 3DES encryption



VPN technologies in Windows Server 2003/Windows XP (cont.)

- Authentication protocols
 - MS-CHAP, MS-CHAP v2
 - Extensible Authentication Protocol (EAP)-based authentication methods
 - EAP-Transport Layer Security (TLS)
- Authentication, Authorization, and Accounting (AAA) support
 - Windows or RADIUS

VPN technologies in Windows Server 2003/Windows XP (cont.)

- Centralized configuration of VPN “connectoids” in the Network Connections folder
 - Connection Manager
 - Connection Manager Administration Kit (CMAK)
 - Client Dialer
 - Connection Point Services
- Access control
 - Network Access Quarantine Control
 - Listener component on the VPN server
 - Notifier component on the VPN client
 - Script run as post-connect action to perform system health checks

VPN technologies in Windows Server 2008/Windows Vista

- New VPN protocol
 - Secure Socket Tunneling Protocol (SSTP)
- Changes to authentication protocols
 - MS-CHAP removed
 - Protected EAP (PEAP)-based authentication methods added
 - PEAP-MS-CHAP v2 and PEAP-TLS
- Changes to access control
 - Network Access Protection (NAP)
 - VPN enforcement method

Protected EAP (PEAP)

- Problem: EAP authentication exchange is sent as plaintext
 - Occurs before encryption starts
 - Password-based EAP exchanges subject to capture and offline dictionary attacks
- PEAP is an EAP type that creates a secure TLS channel between the VPN client and the VPN or RADIUS server
 - TLS channel encrypts subsequent VPN client authentication
 - Allows password-based EAP methods
- One-way certificate authentication
 - VPN client verifies the certificate of the VPN or RADIUS server
 - Buy a third-party certificate

PEAP-MS-CHAP v2

- MS-CHAP v2 EAP type is used after the PEAP TLS channel is created
- Two phase authentication process:
 1. PEAP authentication creates encrypted TLS channel
 2. MS-CHAP v2 authentication exchanges challenges and responses to authenticate VPN client and the VPN or RADIUS server (mutual authentication)

VPN technologies in Windows Server 2008/Windows Vista (cont.)

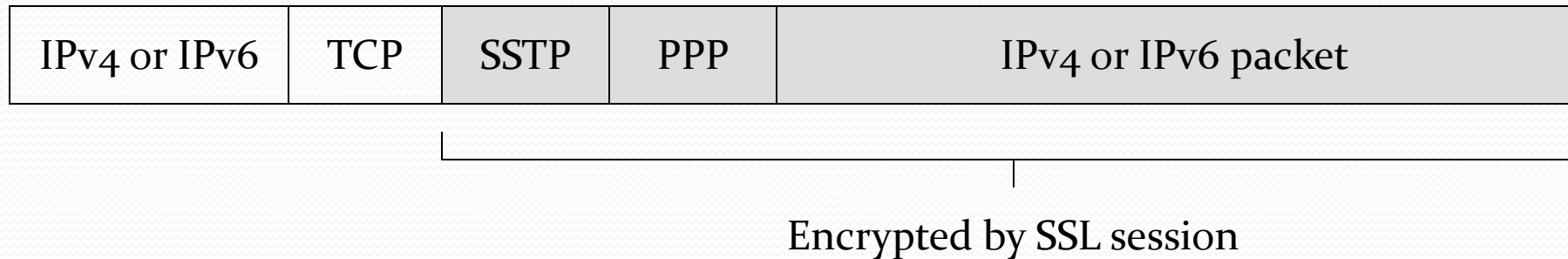
- New IPv6 support
 - Built in to remote access client and server services
 - Types of traffic
 - Over the IPv4 Internet
 - IPv4-encapsulated IPv6 traffic over a VPN tunnel
 - Native IPv6 traffic over a VPN tunnel
 - Over the IPv6 Internet
 - IPv4-encapsulated IPv6 traffic over a VPN tunnel
 - Native IPv6 traffic over a VPN tunnel

VPN technologies in Windows Server 2008/Windows Vista (cont.)

- Changes to cryptographic support
 - L2TP/IPsec
 - Advanced Encryption Standard (AES) with 128 and 256-bit keys.
 - Weaker cryptographic algorithms—40 and 56-bit MPPE for PPTP and DES with MD5 for L2TP/IPsec—are disabled by default (registry setting)
 - Additional certificate checking for L2TP/IPsec connections
- Changes to Connection Manager
 - Multiple-locale support
 - DNS dynamic update

SSTP

- PPTP and L2TP/IPsec might not work behind
 - Firewall/NAT
 - Proxy server
- Windows Vista Service Pack 1 and later
- SSTP uses an HTTPS session with RC4 or AES



VPN technologies in Windows Server 2008 R2/Windows 7

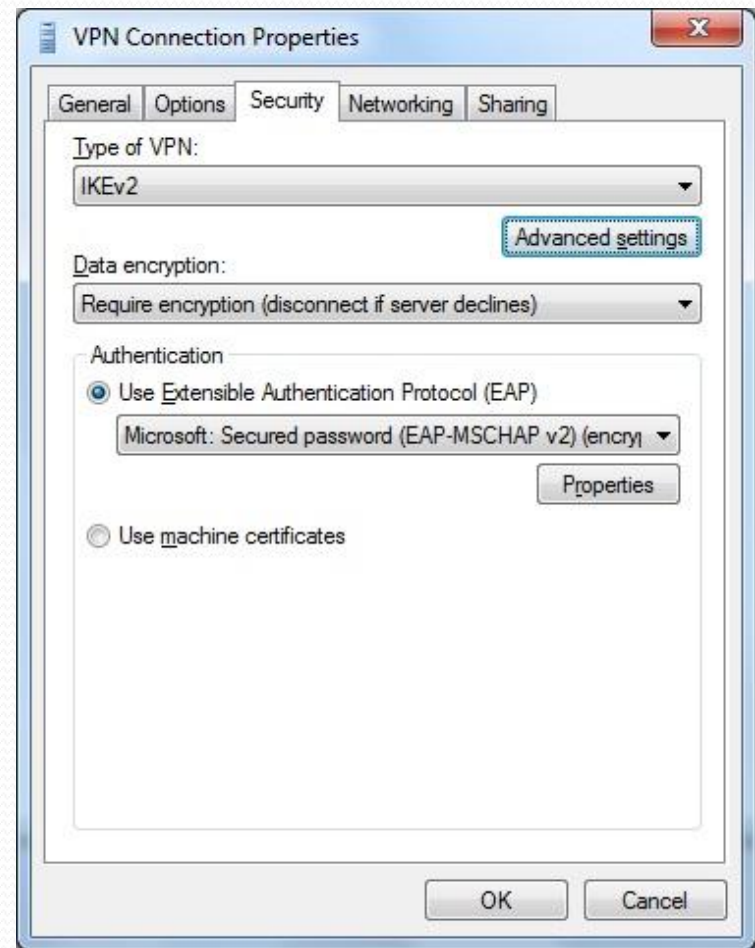
- VPN Reconnect
 - Provides seamless and consistent VPN connectivity when Internet connectivity is temporarily lost
 - Automatically re-establishes the VPN connection
 - Transparent to the user and application
- 2 sets of addresses
 - Inside the tunnel addresses
 - Applications bind to and use
 - Tunnel endpoint addresses
 - Can be temporarily lost or can change and not bring down the entire VPN connection

How VPN Reconnect Works

- Combination of
 - IPsec tunnel mode
 - Internet Key Exchange version 2 (IKEv2)
 - IKEv2 mobility and multihoming extension (MOBIKE)
- Can recover from
 - Frequent disconnections (lossy WWAN connection)
 - Loss of an interface
 - Change in IPv4 or IPv6 address
 - Switch from IPv4 to IPv6 addresses
 - Switch from Internet to intranet

Setting up VPN Reconnect

- On the VPN client, select **IKEv2** as the type of VPN on the **Security** tab
- Select EAP-based authentication or the use of a machine (computer) certificate
- VPN server requires a certificate with the Server Auth EKU





Questions or comments

Resources

- [Windows Server Networking on TechNet](#)
- [Windows Server Networking on MSDN](#)
- [Windows Networking Writing Team blog](#)
- [Windows Server Documentation Twitter feed](#)