Enterprise Security Perimeter Arch

Core Security Services

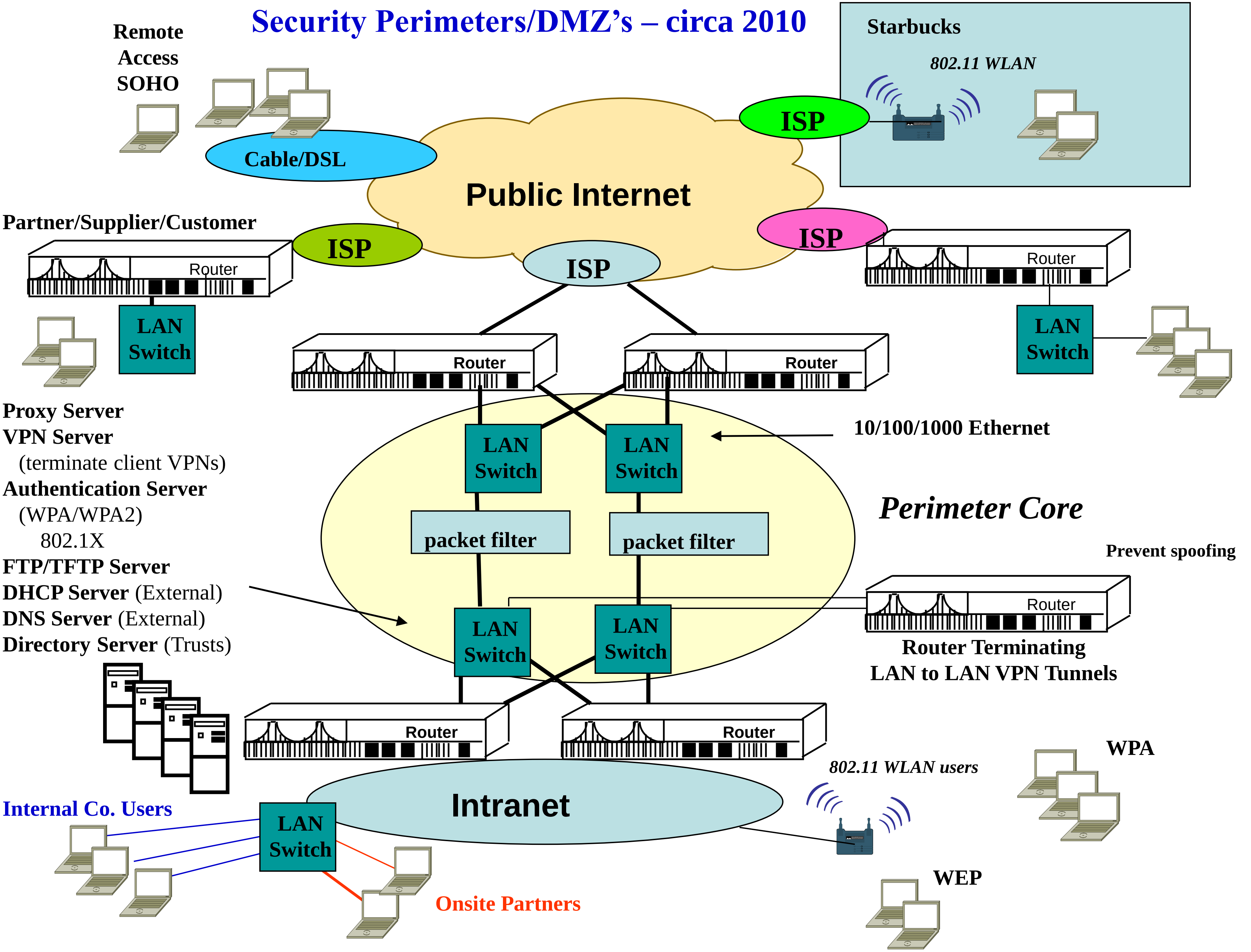
James Farricker

January, 2016

Network/Security Services

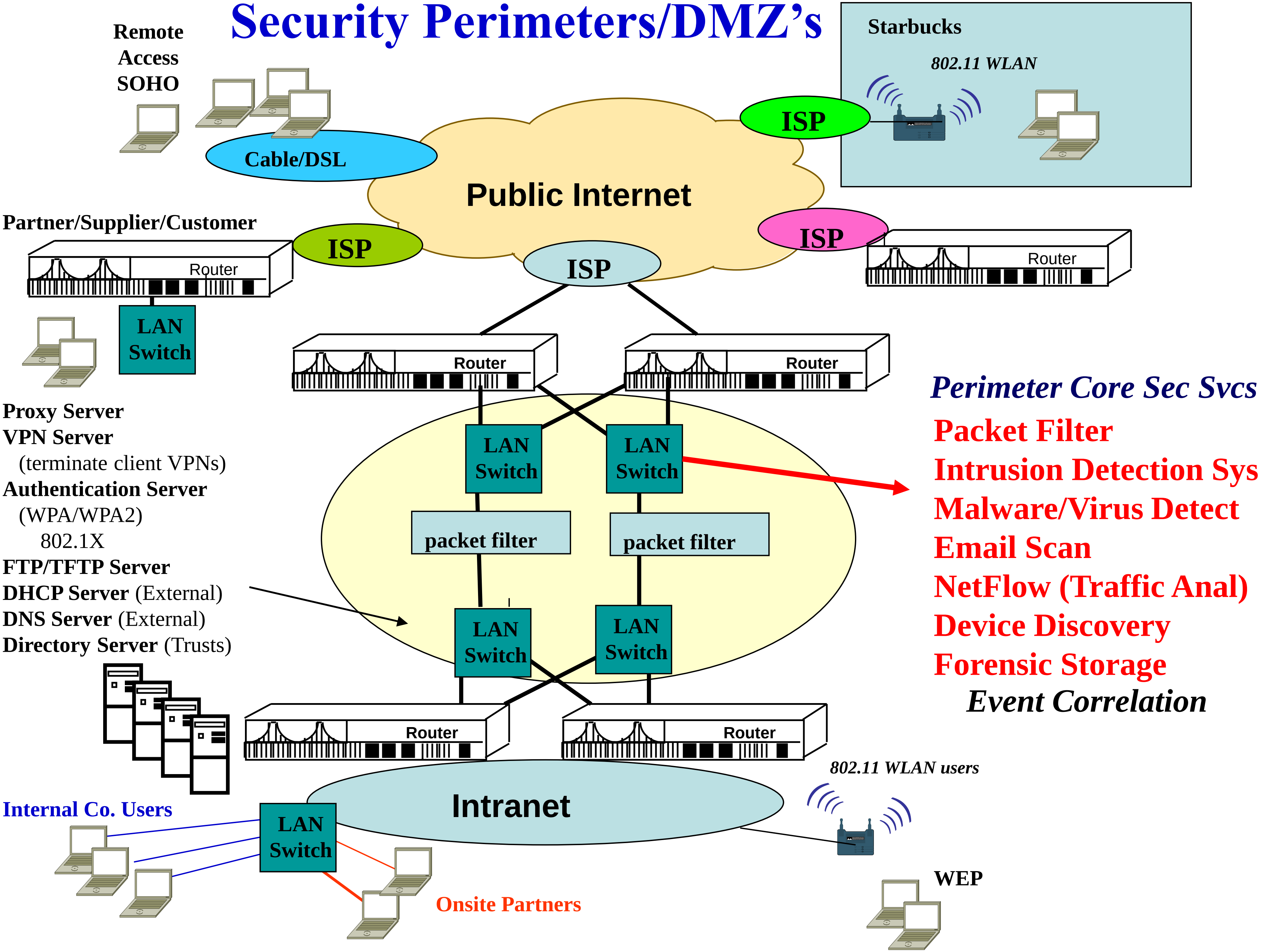
DNS	Domain Name Service
DHCP	Dynamic Host Configuration Protocol
Multicast	SM, DM, SSM
QoS	Quality of Service
GSLB/SLB	Global/Server Load Balancing
NTP	Network Time Protocol
WWW-Proxy	World Wide Web Proxy Service
WINS	Windows Internet Name Service (MS)
DDNS/AD	Dynamic Domain Name Service (MS)
AAA/Security	Authentication, Authorization, Admittance
IPSec	Inbound/Outbound Access
LDAP Directory	Lightweight Directory Access Protocol

Security Perimeters/DMZ's – circa 2010



Proxy Server
VPN Server
(terminate client VPNs)
Authentication Server
(WPA/WPA2)
802.1X
FTP/TFTP Server
DHCP Server (External)
DNS Server (External)
Directory Server (Trusts)

Security Perimeters/DMZ's



Proxy Server
VPN Server
(terminate client VPNs)
Authentication Server
(WPA/WPA2)
802.1X
FTP/TFTP Server
DHCP Server (External)
DNS Server (External)
Directory Server (Trusts)

Internal Co. Users

Onsite Partners

Perimeter Core Sec Svcs

Packet Filter
Intrusion Detection Sys
Malware/Virus Detect
Email Scan
NetFlow (Traffic Anal)
Device Discovery
Forensic Storage
Event Correlation

Security Devices/Components on Perimeter

IDS	***Intrusion Detection System***
Virus/Malware Detect	***Detect signatures of virus/malware in flows***
Device Discovery	***Detects new devices as they activate on net/LAN***
Anomaly Detection	***of traffic flows/patterns***
Proxy Server	***content filtering web proxy server provide admin control over content relayed both directions through the proxy. Ensures acceptable Internet usage.***
Filter/Firewall	***Block/permit IP addresses, TCP/UCP ports***
Correlation Agent	***Fusion/correlation of different security "events"*** ***Security Event Mgmt***

Why would NTP be a critical service ??