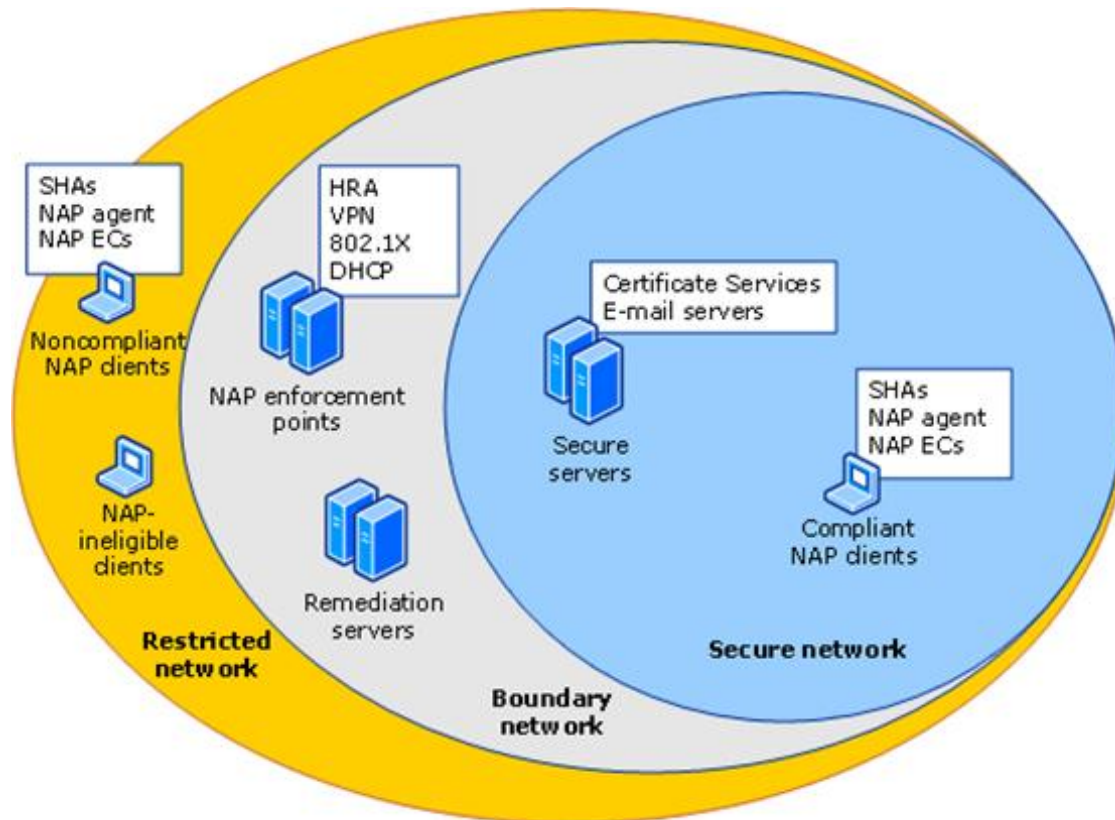


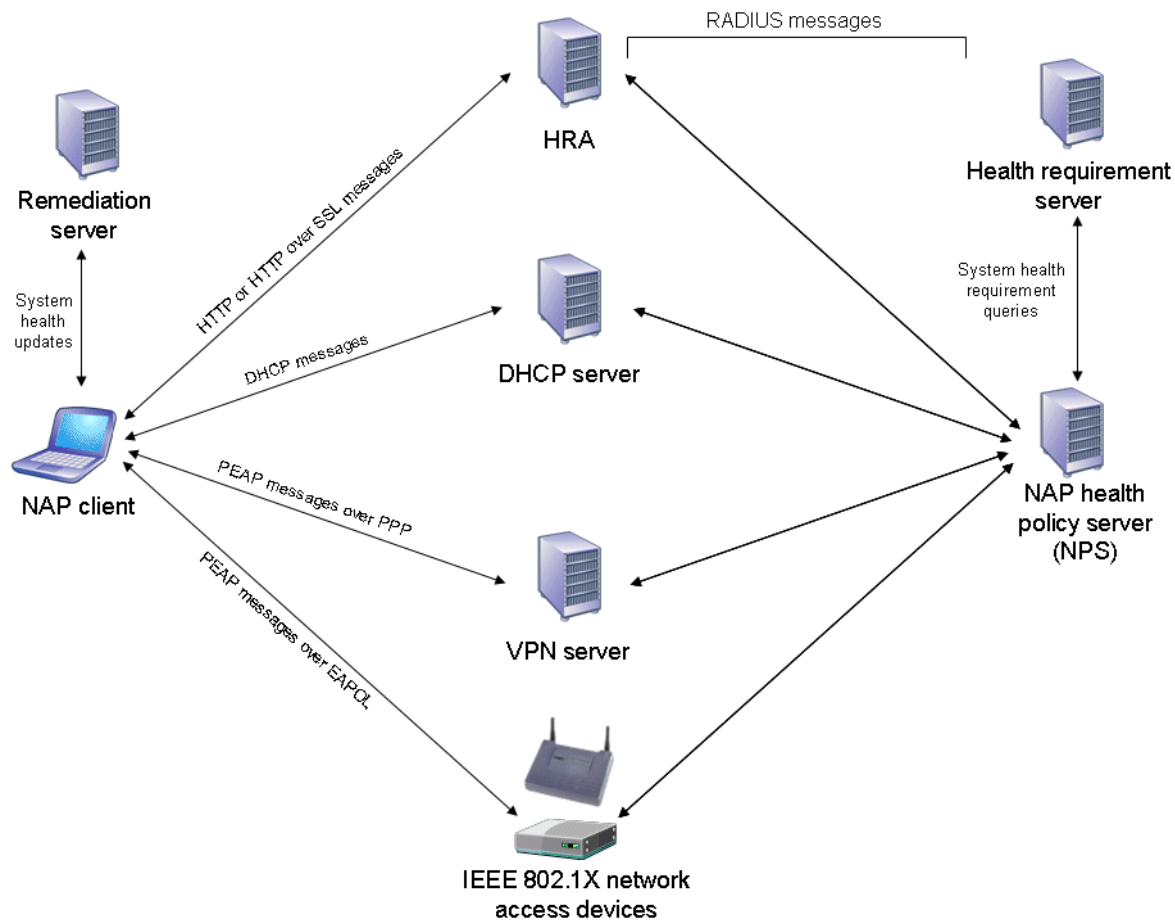
Microsoft NAP Protocols

- Promote Clients from Restricted to Secure Network
 - Based on current Security Policies and Statement of Health
 - NAP failure provides client with address of remediation servers
- Protocol Specifications
 - <http://msdn.microsoft.com/en-us/library/cc216517.aspx>
 - Windows Communication Protocols
 - Windows Server Protocols

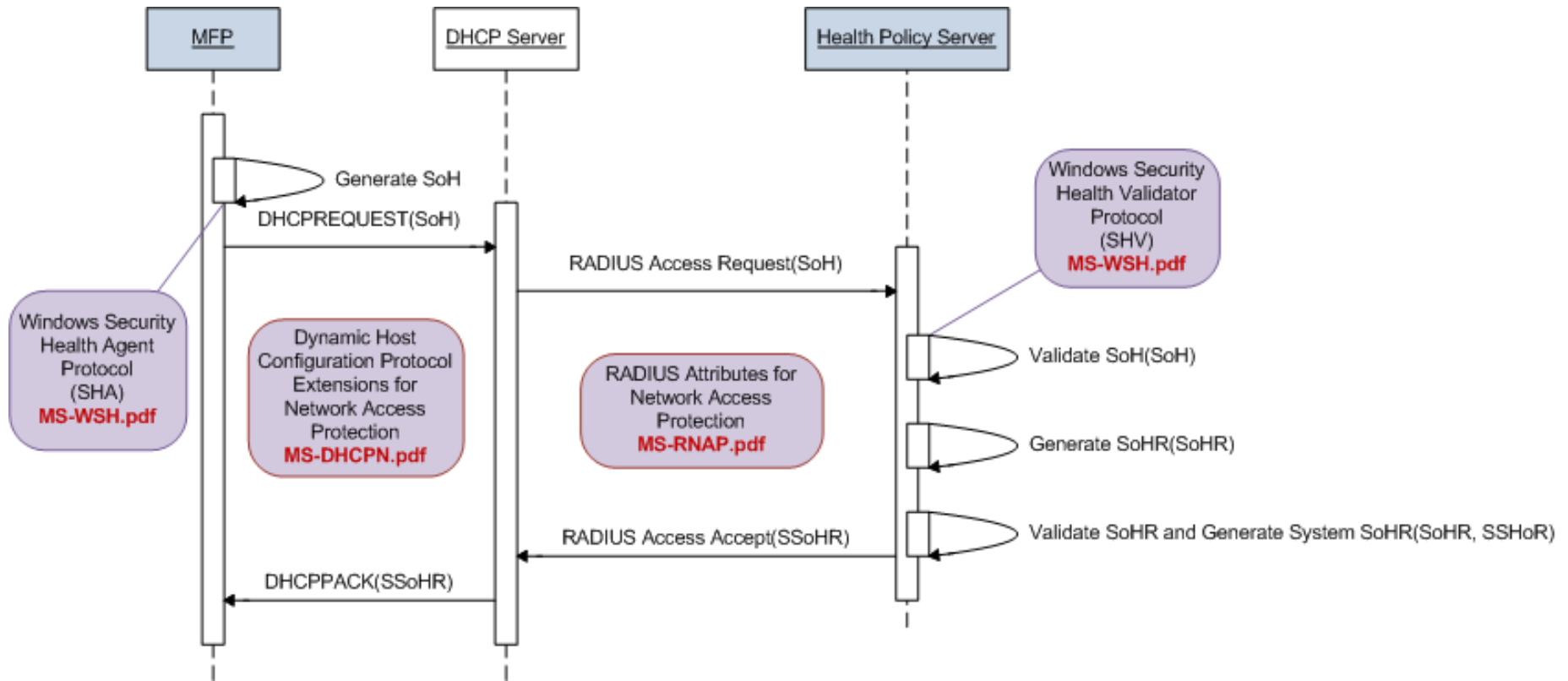


Microsoft NAP Protocols

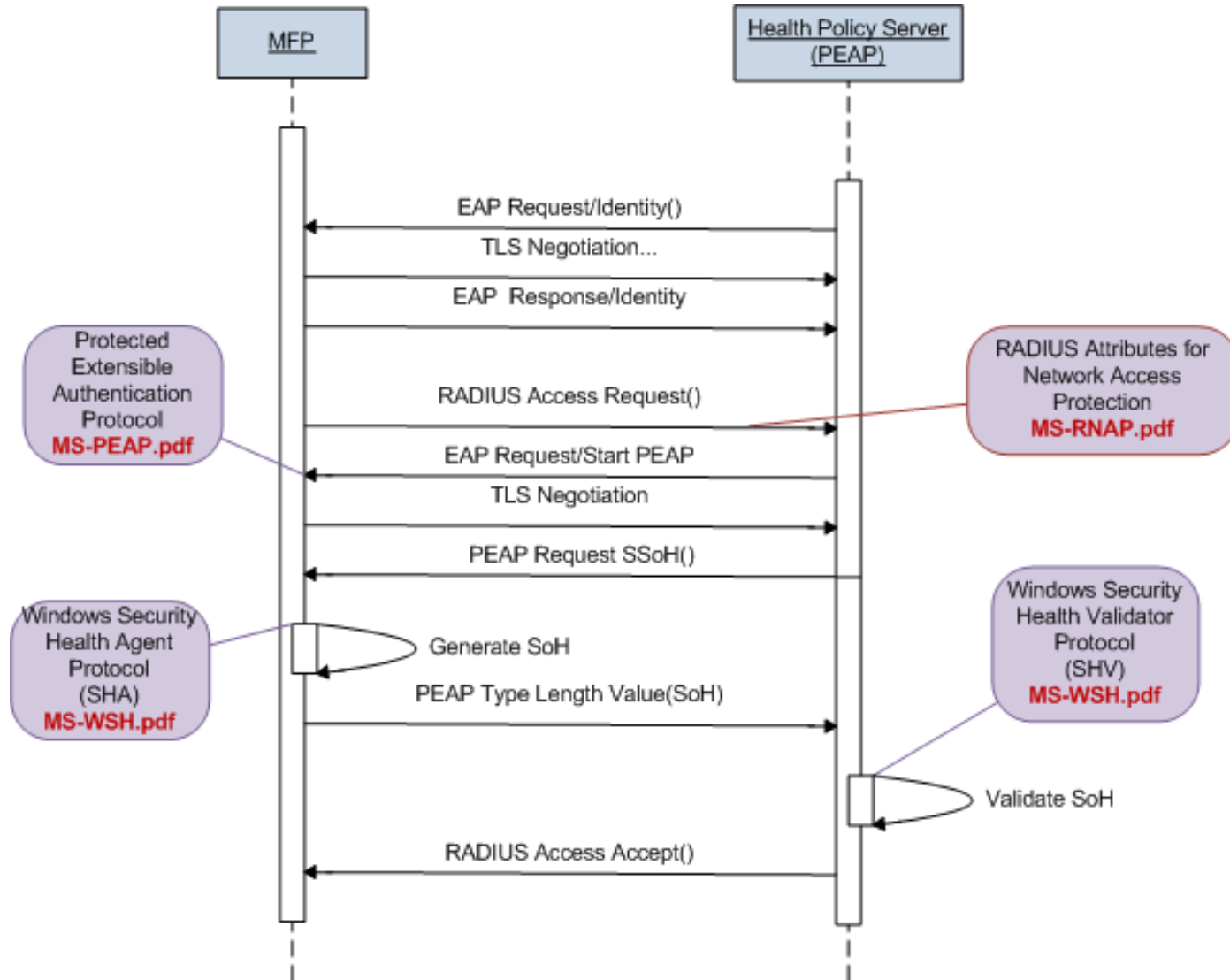
- Support Multiple Access Control Methods
 - DHCP (RADIUS)
 - 802.1x (PEAP - Protected Extensible Enrollment Protocol)
 - VPN (PEAP)
 - IPSec (HCEP – Health Certificate Enrollment Protocol)



NAP DHCP



NAP 802.1x (PEAP)



NAP IPsec (HCEP)

Health Certificate Enrollment Protocol over HTTP/HTTPS transport
MS-HCEP.pdf

URL to HRA must be known:
1) Part of Trusted Server Group in Group Policy settings:
Computer Configuration\Windows Settings\Security Settings\
Network Access Protection\NAP Client Configuration
2) DNS SRV record:
_hra._tcp.site_name._sites.domain_name

HTTP POST
Content-Type: application/healthcertificate-request
Pragma: no-cache
HCEP-Version: 1.0
HCEP-Correlation-Id: <Base64 encoded SOH MS-CorrelationId value>

HTTP Body
ASN.1 encoded PKCS #10 request
PKCS Attributes:
Extended Key Usage
Health Certificate Request OID (1.3.6.1.4.1.311.47.1.1)
id-kp-clientAuth OID (if HRA authentication to Windows Domain)
Subject Alternative Name (FQDN of client)
Statement of Health Certificate Extension
ASN-1 encoded SoH
Cryptographic Service Provider Certificate Extension:
Crypto Service Provider used to generate key pair

Optional Boolean flag (internal) to request client authentication

