Einsatz von 802.11 (Wireless LAN) mit Windows XP und Windows 2000 IAS

Ziel:

- Wireless Client mit Windows XP Professional
- Windows 2000 IAS Server für die RADIUS Authentifizierung
- Wireless Access Point (AP) mit Unterstützung der 802.11 Authentifizierung

Voraussetzung:

- Windows 2000 SP2
- Ein Patch für IAS (Q304697)
- Ein Patch für AD (Q304697)
- Ein Patch für Schannel (Q304347)

Für eine erfolgreiche Authentifizierung benötigt der Wireless Client ein Computer-Zertifikat oder ein Benutzer-Zertifikat oder Beides. Computer mit Windows XP können EAP-TLS verwenden.

Das Computer-Zertifikat wird während des Aufbaus einer EAP-TLS Sitzung abgerufen. Es steht für jeden Benutzer zur Verfügung und auch während des Logons des Computers.

Das Benutzer-Zertifikat ist nur verfügbar wenn der Benutzer sich erfolgreich angemeldet hat, weil nur dann Zugriff auf den persönlichen Zertifikatsspeicher besteht.

Ohne ein Computer-Zertifikat kann der Wireless Client nicht authentifiziert werden

Die Computer und Benutzer-Authentifizierung in Windows XP für Wireless-Clients unterliegt folgender Einschränkung:

- Wenn ein Computer-Zertifikat vorhanden ist wird eine Computer-Authentifizierung durchgeführt
- Wenn die Computer-Authentifizierung durchgeführt wurde, wird keine User-Authentifizierung nach der Computer-Authentifizierung durchgeführt.
- Wenn der Benutzer-Logon erfolgreich war und der Benutzer auf den Wireless AP geschaltet wird, wird die Benutzer-Authentifizierung durchgeführt
- Wenn kein Computer-Zertifikat existiert oder die Benutzer-Authentifizierung war erfolgreich vor der Computer-Authentifizierung wird die Benutzer Authentifizierung durchgeführt

Gängige Infrastruktur

- Wireless Computer mit Windows XP
- Zwei Windows 2000 IAS Server

- Active Directory Domänen
- Eine PKI
- Wireless Remote Access Policy
- Mehrere Wireless Access Points (AP)

Verwendung einer Third Party CA

Für Zertifkate auf dem IAS Server

- Zertifikate müssen im lokalen Zertifikatsspeicher des Computers installiert sein
- Zertifikate müssen über einen privaten Schlüssel verfügen
- Der CSP muß Schannel unterstützen
- Die PKI muß das Server Authentifizierungs-Zertifikat enthalten. Auch bekannt als Enhanced Key Usage (EKU). EKU wird durch eine OID identifiziert (1.3.6.1.5.7.3.1)
- Sie muß einen FQDN des Computer-Accounts im IAS (alternativer Name im Subjekt) enthalten.
- Das Root CA Zertifikat der CA welches das Wireless Computer- und Benutzerzertifikat ausstellt muß im Zertifikatsspeicher der „Trusted Root Certificate Authority“ gespeichert sein.

Für Zertifikate auf dem Wireless Client

- Der Benutzer muss über einen korrospondierenden privaten Schlüssel verfügen
- Es muß die EKU (OID 1.3.6.1.5.5.7.3.2) enthalten sein
- Computer Zertifikate müssen in dem lokalen Computer-Zertifikats-Speicher installiert sein
- Computer-Zertifikate müssen den FQDN des Wireless Client Computer Accounts enthalten
- Benutzer-Zertifkate müssen im Benutzer-Zertifkatsspeicher installiert sein
- Benutzer-Zertifikate müssen den UPN des Computer Accounts im „Alternative Name Property“ enthalten
- Das Root CA Zertifikat der Cas für den IAS Server muß im Zertifkatsspeicher der „Trusted Root Certification Authority“ installiert sein

Installation des IAS Servers

- SECEDIT /REFRESHPOLICY MACHINE_POLICY
- Installation von IAS
- Neuinstallation von Windows 2000 SP2
- Installation des Patches Q304697
- IAS im AD registrieren
- Aktivieren des Datei-Loggings im IAS
- Evtl. Konfiguration zusätzlicher UDP Ports für die Authentifizierung und das Accounting (Standard = Port 1812 und 1645 für Authentifzierungs-Nachrichten und Port 1813 und 1646 für Accouning-Nachrichten)
- Hinzufügen der Wireless APs als IAS Clients
- Erstellen einer neuen RAS Policy mit den folgenden Einstellungen:
  Name: Wireless Zugriff in das Internet
  Konditionen: NAS-Port-Typ=Wireless oder Wireless-IEEE 802.11

Windows-Gruppe=WirelessBenutzer
Berechtigungen: RAS Zugriff erlauben

- Benutzer-Profil-Authentifizierung=EAP und SmartCard oder anderes Zertifikat auswählen
- Benutzer-Profil-Verschlüsselung=Stärkste Verschlüsselung (128 Bit)
- Löschen der Default-Domain Policy

Installation des sekundären IAS Servers

- SECEDIT /REFRESHPOLICY MACHINE_POLICY
- Installation von IAS
- Neuinstallation von Windows 2000 SP2
- Installation des Patches Q304697
- IAS im AD registrieren
- Kopieren der IAS Konfiguration des ersten IAS auf den zweiten IAS
  NETSH AAAA SHOW CONFIG >Pfad zur Datei.txt auf dem ersten IAS ausführen
  NETSH EXEC >Pfad zur Datei.txt (des ersten IAS Servers) auf dem zweiten IAS Server ausführen

Installation des Computer-Zertifikats auf dem Wireless Client

- Konfiguration einer Gruppenrichtlinie mit automatischen Zertifikats-Enrollment.
- Den Wireless Client an das Intranet anschließen
- Auf dem Client GPUPDATE /TARGET:COMPUTERNAME ausführen (wenn es sich um einen Windows XP Client handelt)

Installation des Benutzer-Zertifikats auf dem Wireless Client

- Erstellen eines Benutzer-Zertifikats mit dem beabsichtigten Zweck für den Benutzer
- Exportieren des Zertifikats in eine .CER Datei
- Mappen des .CER Zertifikats zu dem Benutzer Account der das Wireless Gerät nutzen soll
- Exportieren des Benutzer-Zertifikats in eine .PFX-Datei. Exportieren des privaten Schlüssels und Speicherung auf mehrere Disketten und anschließender Löschung des privaten Schlüssels
- Importieren des Benutzer-Zertifkats auf dem Wireless Client