Best Practices
WPA2 Enterprise und Radius-SSO

Jonas Spieckermann
Senior Sales Engineer

Jonas.Spieckermann@watchguard.com

Grundlage WLAN

- IEEE 802.11 definiert den Standard für Wi-Fi Netze
- 2 Frequenzbänder 2.4 GHz und 5 GHz werden genutzt
  - 2.4 GHz = 14 Kanäle
    - Definiert in den Standards 802.11 B/G/N
  - 5 GHz = 23 Kanäle
    - Definiert in den Standards 802.11 A/N/AC
- Verschiedene Verschlüsselungen und Sicherheitseinstellungen
  - Open System = keine Verschlüsselung
  - WEP
    - veraltet und unsicher aber dennoch im Einsatz
  - WPA/WPA2
    - PSK oder Radius basierte Authentifizierung (WPA Enterprise)
    - TKIP oder AES

Grundlagen WPA2 Enterprise

- Definiert in IEEE 802.1x
- Verwendung eines Radius Servers
- Accesspoint als “Authenticator“
  - “vermittelt“ zwischen Client und Radius Server
- Zugriff zum Wi-Fi Netz nur, wenn der Radius Server die Anmeldung bestätigt

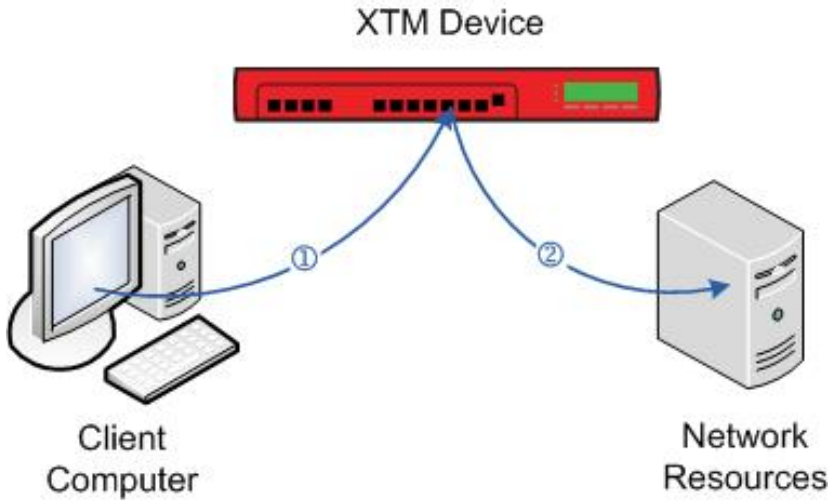
Vorteile durch WPA2 Enterprise

- Kein gemeinsam genutzter Preshared Key
- Persönlicher Zugang
  - Kann pro Nutzer verwaltet und deaktiviert werden
- Unterstützt auch Client Zertifikate
  - „Geräteabhängige Authentifizierung“

Grundlagen Authentifizierung

Warum wird eine Benutzerauthentifizierung benötigt?

- Dynamische IP Addressierung (DHCP)
- Anwender nutzen mehrere Geräte gleichzeitig
- Terminal Server
- Darstellung in Log-Meldungen / Reports
- wechselnde Systeme der Mitarbeiter
- Gruppenspezifische Zugriffe
- Definition von Ausnahmen
- ....



① — User enters user name and password from the client computer.
② — XTM Device authenticates user and allows the user to connect to resources on the network.

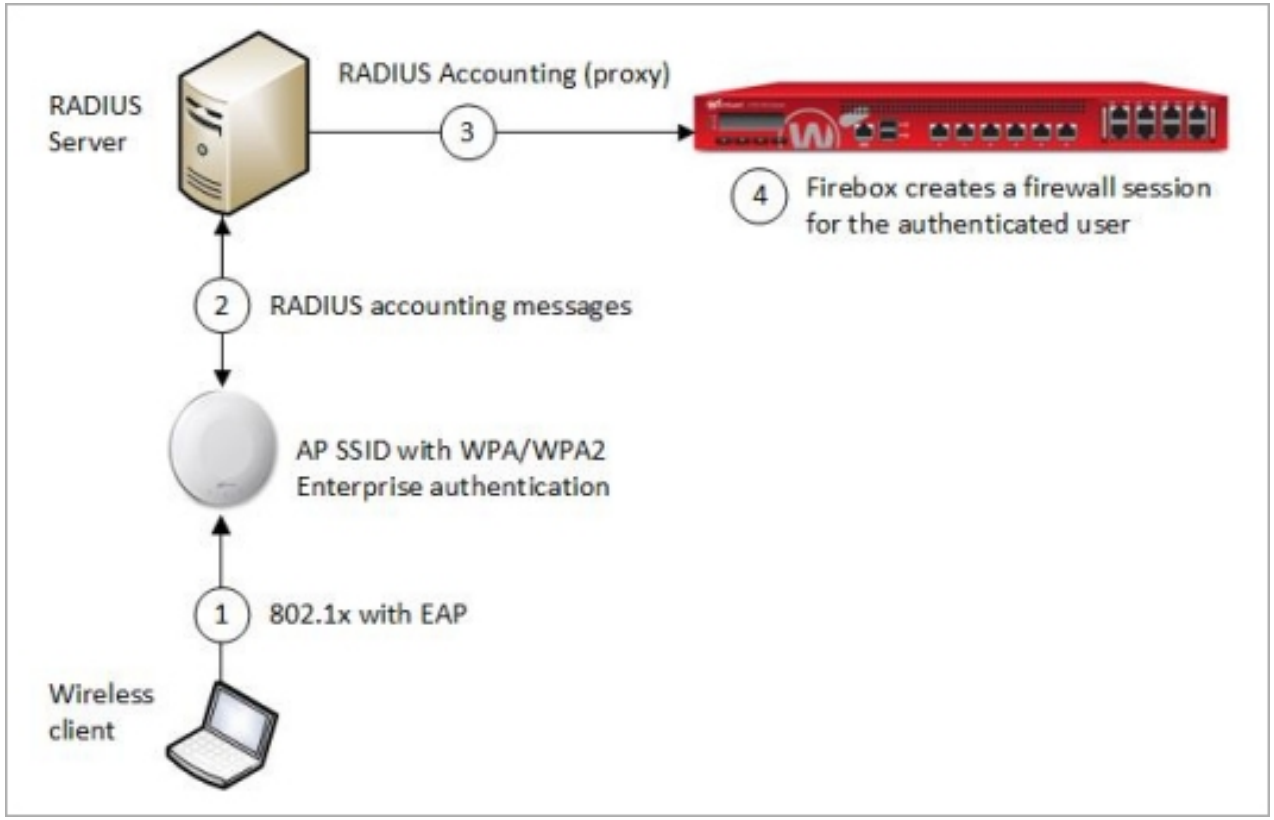
Grundlagen SSO

- Die Authentifizierung soll ohne manuelle Aktion des Anwenders erfolgen.
- „Anmeldung am Betriebssystem -> Firebox kennt den User“

- WatchGuard Single Sign-On ist flexible nutzbar:
  - SSO Agent, SSO Client, Exchange Monitor, Eventlog Monitor und Radius SSO




Radius Single Sign-On für WPA2 Enterprise



RADIUS SSO - Anforderungen

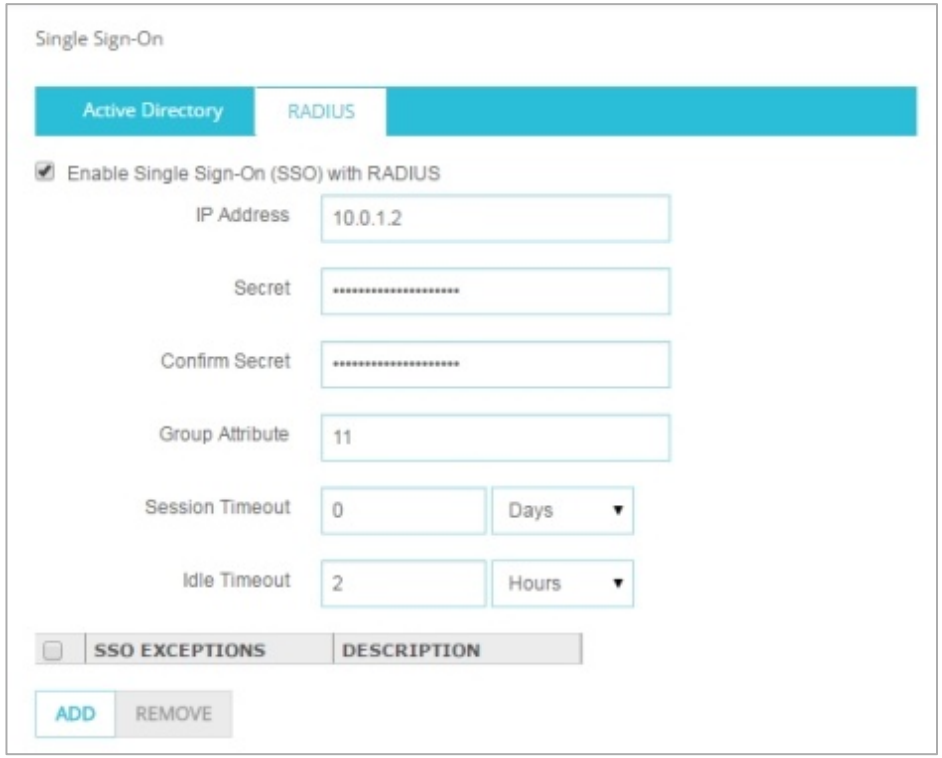
- Wireless Accesspoints müssen 802.1x Authentication und RADIUS Accounting unterstützen.

- **Start**, **Stop** und **Interim-Update** RADIUS Accounting Nachrichten müssen die folgenden Attribute enthalten:
  - **User-Name** — Name des angemeldeten Nutzers
  - **Framed-IP-Address** — IP Adresse des Systems

- Ein RADIUS Proxy System (Funktion des RADIUS Server) muss bei Verwendung von mehreren Accesspoints Accounting Meldungen an die Firebox weiterleiten.

Konfiguration von RSSO

- Web UI — **Authentication > Single Sign-On > RADIUS**
  - RSSO kann für eine RADIUS server IP address aktiviert werden
  - **Group Attribute** dient der Verwendung eigener Gruppen
  - Group Attribute muss der Filter-ID innerhalb des RADIUS server entsprechen (Rückgabewert).



RSSO - Gruppen und Policies

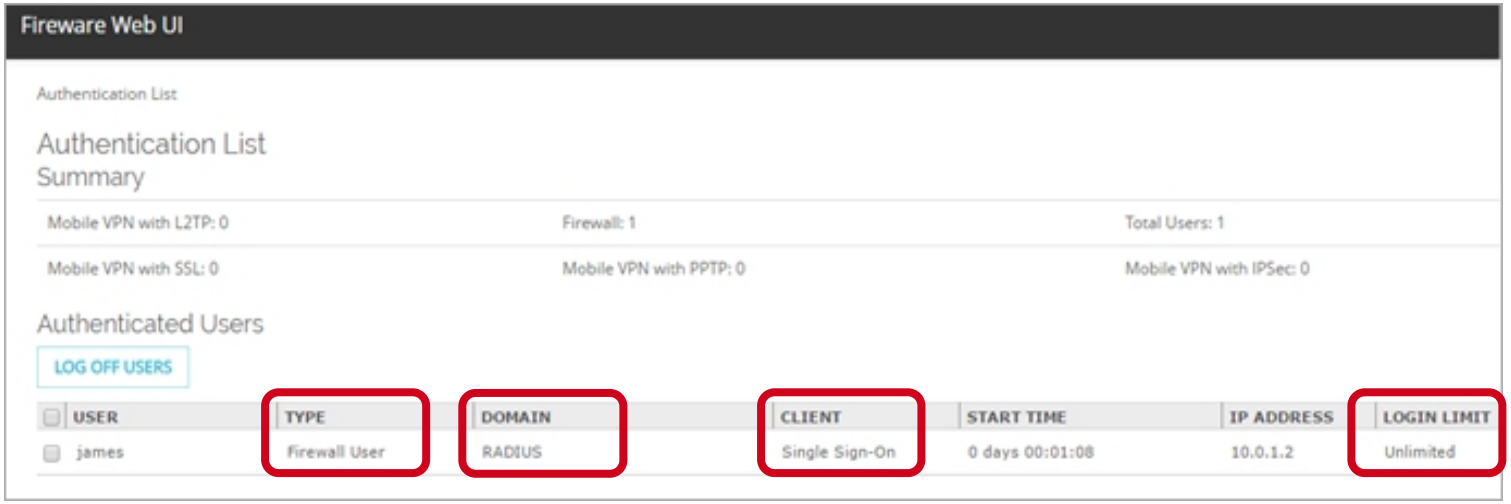
- Wird RSSO aktiviert, so wird automatisch die Gruppe **RADIUS-SSO-Users** eingerichtet
  - RSSO unterstützt auch selbst definierte Gruppen, die im RADIUS System und der Firebox konfiguriert werden.
  - RSSO Nutzer, die nicht einer selbst definierten Gruppe angehören, werden zu **RADIUS-SSO-Users** zugeordnet.

RSSO — Gruppen und Policies

- Bei Einrichtung von RSSO werden die folgenden Firewall-Policies automatisch angelegt
  - **Allow RADIUS SSO Service**
    - Erlaubt eingehende Kommunikation auf port 1813 zur Firebox (RADIUS Accounting).
  - **Allow RADIUS SSO Users**
    - Erlaubt ausgehende Kommunikation der authentifizierten Nutzer
    - TCP-UDP Datenverkerh der **RADIUS-SSO-Users** zu **Any-External** ist freigegeben.
- Für selbst definierte Gruppen sollten eigene Firewall Policies erzeugt werden.

RSSO — Session Status

- Angemeldete Nutzer werden in der **Authentication List** dargestellt
  - **Type** — Firewall User
  - **Domain** — RADIUS
  - **Client** — Single Sign-On
  - **Login Limit** — Based on the user/group login limit



RSSO und Active Directory Single Sign-On

- RSSO und Active Directory Single Sign-On können parallel verwendet werden.
- RSSO überschreibt vorhandenen Acitve Directory SSO Sessions nicht
- Wir empfehlen Ausnahmen für Netzbereiche in denen RSSO genutzt wird zu definieren, sodass AD SSO in diesen Subnetzen nicht angewendet wird.
- Ausnahmen können über die “Exception List” auch pro IP-Adresse / IP-Range definiert werden.

Radius SSO Live

WPA2 Enterprise mit WatchGuard AP320
Radius Server: Microsoft NPS on Windows Server

Vielen Dank

Jonas Spieckermann
Senior Sales Engineer

Jonas.Spieckermann@watchguard.com