



Best Practices - Single Sign ON - User basierte Autorisierung an der WatchGuard Firewall

Thorsten Steding
Sales Engineer

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



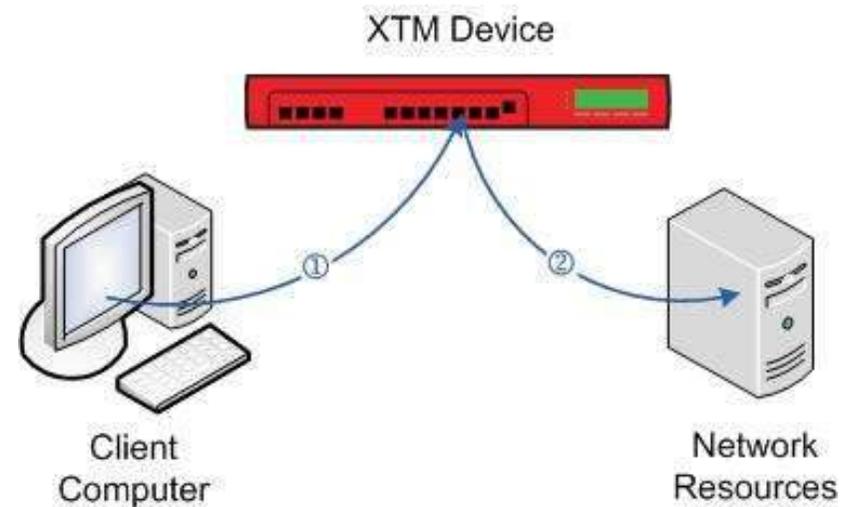
Vorteile durch WPA2 Enterprise

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

Grundlagen Authentication

Warum wird eine Benutzerauthentifizierung benötigt?

- Dynamische IP Adressierung (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

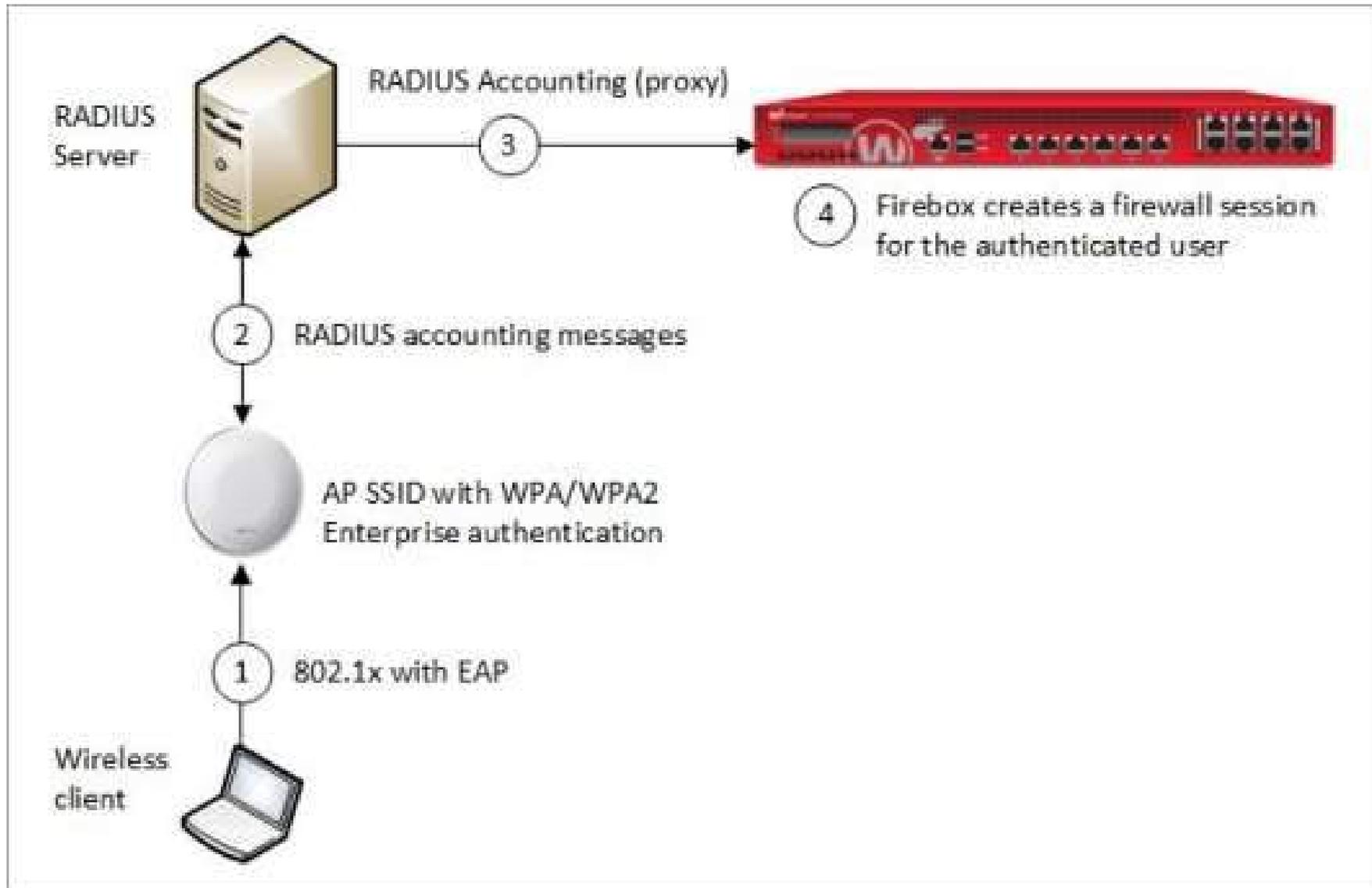
- Die Authentifizierung soll ohne manuelle Aktion des Anwenders erfolgen.
- „Anmeldung am Betriebssystem -> Firebox kennt den User“
- WatchGuard Single Sign-On ist flexible nutzbar:
 - SSO Agent, SSO Client, Exchange Monitor, Eventlog Monitor und Radius SSO



iOS



RSSO — How it Works



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.

Configure RSSO on the Firebox

- Web UI — **Authentication > Single Sign-On > RADIUS**
 - Sie können RSSO für eine RADIUS-Server-IP-Adresse aktivieren
 - **Group Attribute** ist für benutzerdefinierte Gruppen
 - Es muss mit dem Filter-ID-Attribut für die Gruppe auf dem RADIUS-Server übereinstimmen

The screenshot shows the 'Single Sign-On' configuration page in the WatchGuard Web UI. The 'RADIUS' tab is selected. The 'Enable Single Sign-On (SSO) with RADIUS' checkbox is checked. The configuration fields are as follows:

- IP Address: 10.0.1.2
- Secret: [Redacted]
- Confirm Secret: [Redacted]
- Group Attribute: 11
- Session Timeout: 0 Days
- Idle Timeout: 2 Hours

Below the fields is a table for 'SSO EXCEPTIONS' with a 'DESCRIPTION' column. At the bottom are 'ADD' and 'REMOVE' buttons.

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 Datenverkehr der **RADIUS-SSO-Users** zu **Any-External** ist freigegeben.
- Für selbst definierte Gruppen sollten eigene Firewall Policies erzeugt werden.

RSSO — Session Status

- Über RSSO authentifizierte Benutzersitzungen erscheinen in der Authentifizierungsliste
 - **Type** — Firewall User
 - **Domain** — RADIUS
 - **Client** — Single Sign-On
 - **Login Limit** — Based on the user/group login limit

Fireware Web UI

Authentication List

Authentication List Summary

Mobile VPN with LZTP: 0	Firewall: 1	Total Users: 1
Mobile VPN with SSL: 0	Mobile VPN with PPTP: 0	Mobile VPN with IPsec: 0

Authenticated Users

[LOG OFF USERS](#)

USER	TYPE	DOMAIN	CLIENT	START TIME	IP ADDRESS	LOGIN LIMIT
james	Firewall User	RADIUS	Single Sign-On	0 days 00:01:08	10.0.1.2	Unlimited



Radius SSO Live

WPA2 Enterprise mit WatchGuard AP325
Radius Server: Microsoft NPS on Server 2016
T55-w



Vielen Dank