A large, detailed illustration of a lion's head and shoulders, rendered with a strong red color cast. The lion has a thick, dark mane and is looking slightly to the right with a serious expression. The background is plain white.

Best Practice – Verwendung von WPA2 Enterprise in unterschiedlichen WatchGuard Produkten

Agenda

- Was genau ist RADIUS / WPA2 Enterprise? Für welche Szenarien wird dieser Standard verwendet?
- Wo verwendet WatchGuard RADIUS in seinen Produkten?
- Beispiele von Anwendungen von RADIUS / WPA2 Enterprise innerhalb der WatchGuard Welt
- Live Demo

Was genau ist RADIUS

- *Remote Authentication Dial-In User Service* (RADIUS, deutsch Authentifizierungsdienst für sich einwählende Benutzer) ist ein Client-Server-Protokoll, das zur
 - Authentifizierung,
 - Autorisierung und zum
 - Accounting(Triple-A-System) von Benutzern bei Einwahlverbindungen in ein Computernetzwerk dient.
- RADIUS ist der De-facto-Standard bei der zentralen Authentifizierung von Einwahlverbindungen über Modem, ISDN, VPN, WLAN (IEEE 802.1X) und DSL.

Quelle: Wikipedia (https://de.wikipedia.org/wiki/Remote_Authentication_Dial-In_User_Service)

Was genau ist RADIUS

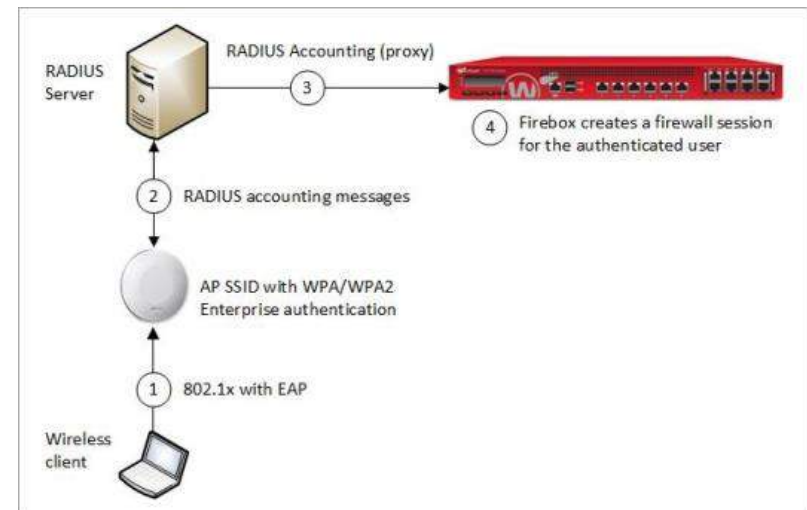
- Ein RADIUS-Server ist ein **zentraler** Authentifizierungsserver, an den sich Services für die Authentifizierung von Clients in einem physischen oder virtuellen Netzwerk (VPN) wenden.
- Der RADIUS-Server übernimmt dabei für den Service die *Authentifizierung*, das heißt die Überprüfung von Benutzername und Kennwort.
- Des Weiteren werden Parameter für die Verbindung zum Client bereitgestellt. Die dabei verwendeten Daten entnimmt der RADIUS-Server eigenen Konfigurationsdateien, eigenen Konfigurationsdatenbanken oder ermittelt diese durch Anfragen an weitere Datenbanken oder Verzeichnisdienste, in denen die Zugangsdaten wie Benutzername und Kennwort gespeichert sind.

Was genau ist WPA2 Enterprise

- Wi-Fi Protected Access 2 (WPA2) ist die Implementierung eines Sicherheitsstandards für Funknetzwerke nach den WLAN-Standards IEEE 802.11a, b, g, n und ac und basiert auf dem *Advanced Encryption Standard* (AES).
- Zur Authentifizierung des Clients am Access Point und umgekehrt können sowohl ein geheimer Text (der pre-shared key, PSK), als auch ein RADIUS-Server verwendet werden.
- Die Authentifizierung mit einem Pre-Shared-Key wird oft bei kleinen Installationen wie bei Privatanwendern üblich benutzt und daher auch als „Personal“ bezeichnet.

Was genau ist WPA2 Enterprise

- In größeren Netzen ermöglicht die Verwendung von RADIUS eine zentrale Benutzeradministration inklusive Accounting.
- Der Access Point leitet in diesem Fall die Authentifizierungsanfrage des Clients an den RADIUS-Server weiter und lässt – je nach Erfolg – den Zugriff zu.
- Diese Variante von WPA2 wird oft als „Enterprise“ bezeichnet.
- Der Access Point ist in diesen Fall der „Authenticator“.



Einsatz Szenarien

- RDAIUS wird für Anmeldungen an VPN Systeme verwendet.
- Weitere Szenarien können aber auch Authentifizierungen an Drittanwendungen sein, z.B. Citrix Netscaler oder WatchGuard Dimension.
- WPA2 Enterprise wird primär im internen Netzwerk für die Authentifizierung an Access Points oder andere Netzwerk Devices eingesetzt. Interessant ist hier die Verwendung eines sog. „Single Sign On“ Verfahren.

Einsatz Szenarien

- In der WatchGuard Welt wird RADIUS verwendet für
 - VPN Einwahl
 - RADIUS SSO
 - Authentifizierung per WPA2 Enterprise (Wi-Fi und Wired)
 - RADIUS Support für WatchGuard AuthPoint
 - RADIUS Anmeldung an einer WatchGuard Firebox
 - RADIUS Anmeldung an WatchGuard Dimension
 - ...



RADIUS SSO mit WatchGuard



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-Adresse aktiviert werden
 - **Group Attribute** dient der Verwendung eigener Gruppen
 - Group Attribute muss der Filter-ID innerhalb des RADIUS Server entsprechen (Rückgabewert).

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

At the bottom, there is a table for 'SSO EXCEPTIONS' with columns for 'SSO EXCEPTIONS' and 'DESCRIPTION'. Below the table are 'ADD' and 'REMOVE' buttons.

RSSO - Gruppen und Policies

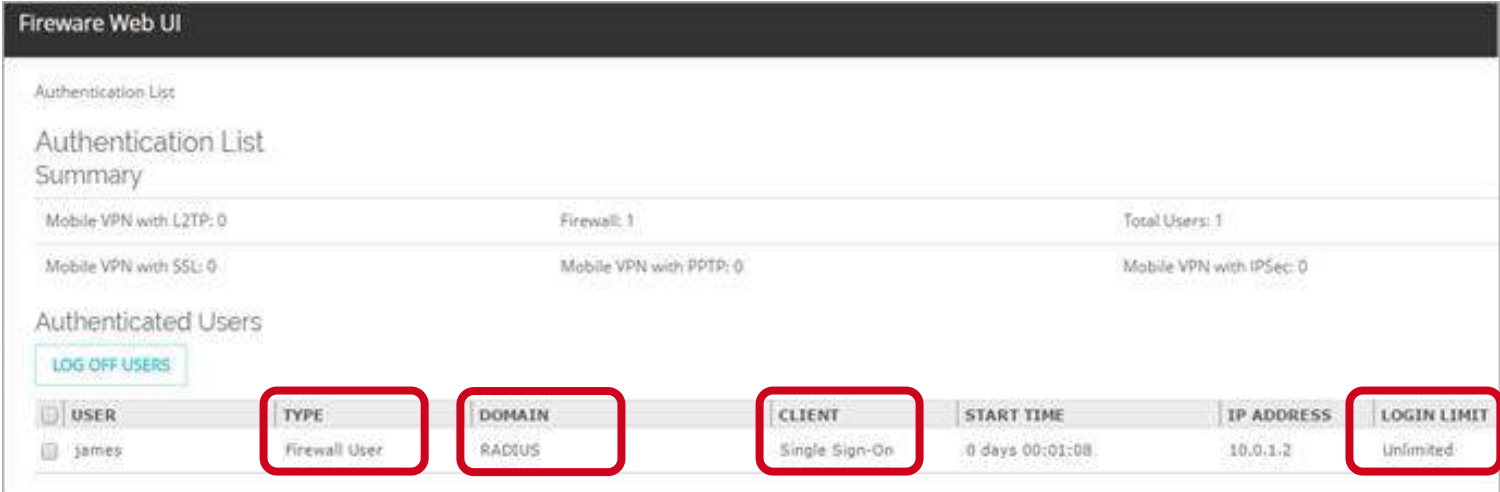
- Wird RSSO aktiviert, so wird automatisch die Gruppe **RADIUS-SSO-Users** eingerichtet
 - RSSO unterstützt auch selbst definierte Gruppen, die im RADIUS System und der Firebox konfiguriert werden.
 - RSSO Nutzer, die nicht einer selbst definierten Gruppe angehören, werden zu **RADIUS-SSO-Users** zugeordnet.

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

- 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



The screenshot shows the 'Authentication List' section in the Fireware Web UI. It includes a 'Summary' section with statistics for Mobile VPN with L2TP, Mobile VPN with SSL, Firewall, Mobile VPN with PPTP, Total Users, and Mobile VPN with IPsec. Below this is the 'Authenticated Users' section, which contains a table of active sessions. The columns 'TYPE', 'DOMAIN', 'CLIENT', and 'LOGIN LIMIT' are highlighted with red boxes. A 'LOG OFF USERS' button is also visible.

USER	TYPE	DOMAIN	CLIENT	START TIME	IP ADDRESS	LOGIN LIMIT
<input type="checkbox"/> james	Firewall User	RADIUS	Single Sign-On	0 days 00:01:08	10.0.1.2	Unlimited

RSSO und Active Directory Single Sign-On

- RSSO und Active Directory Single Sign-On können parallel verwendet werden.
- RSSO überschreibt vorhandenen Active 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.



WPA2 Enterprise Authentifizierung mit WatchGuard APs



WPA2 Enterprise Authentifizierung mit WatchGuard APs

- Um die Enterprise-Authentifizierungsmethoden zu verwenden, müssen Sie einen externen RADIUS-Authentifizierungsserver konfigurieren.
- WatchGuard APs unterstützen drei wireless Authentifizierungsmethoden für WPA und WPA2 Enterprise:
 - WPA Enterprise - Der AP akzeptiert Verbindungen von wireless Geräten, die für die Verwendung der WPA Enterprise-Authentifizierung konfiguriert sind.
 - WPA2 Enterprise - Der AP akzeptiert Verbindungen von wireless Geräten, die für die Verwendung der WPA2 Enterprise-Authentifizierung konfiguriert sind. WPA2 implementiert den vollständigen 802.11i-Standard. Bei einigen älteren WLAN-Karten funktioniert dies nicht.
 - WPA / WPA2 Enterprise - Der AP akzeptiert Verbindungen von wireless Geräten, die für die Verwendung der WPA Enterprise- oder WPA2 Enterprise-Authentifizierung konfiguriert sind.

WPA2 Enterprise Authentifizierung mit WatchGuard APs

- Sie müssen die IP-Adressen Ihrer WatchGuard APs und der Firebox als RADIUS-Clients auf Ihrem RADIUS-Server hinzufügen.
- WatchGuard-APs stellen für Authentifizierungsanforderungen eigene Verbindungen zum RADIUS-Server her.
- Stellen Sie sicher, dass Ihre Firebox als RADIUS-Client für andere Arten der firebox-basierten Authentifizierung hinzugefügt wurde.

WPA2 Enterprise Authentifizierung mit WatchGuard APs

- Einstellung in der SSID für WPA2 Enterprise:
- Wählen Sie in der Dropdown-Liste Sicherheitsmodus die Option WPA Enterprise, WPA2 Enterprise oder WPA / WPA2 Enterprise aus.
 - TKIP oder AES - Verwendet entweder TKIP oder AES zur Verschlüsselung. (Nur WPA- oder WPA / WPA2-Mischmodus). TKIP ist ein veraltetes, unsicheres Protokoll und wird nur im WPA2-Modus nicht unterstützt.
 - AES - Verwendet nur AES (Advanced Encryption Standard) für die Verschlüsselung.

The screenshot shows the configuration page for a SSID named 'Guest-Wireless' in the Security tab. The 'Security Mode' is set to 'WPA/WPA2 Enterprise', and the 'Encryption' is set to 'TKIP or AES'. Other fields include 'Group Key Update Interval' (3600), 'RADIUS Server', 'RADIUS Port' (1812), 'RADIUS Secret', 'Enable RADIUS Accounting' (unchecked), 'RADIUS Accounting Server', 'RADIUS Accounting Port' (1813), 'RADIUS Accounting Secret', and 'Interim Accounting Interval' (600). There is also an option to 'Enable Fast Roaming (802.11k, 802.11r)' which is checked, with a note that it requires WPA2 Enterprise authentication and only applies to AP300 devices. 'SAVE' and 'CANCEL' buttons are at the bottom.

Field	Value
Network Name (SSID)	Guest-Wireless
Security Mode	WPA/WPA2 Enterprise
Encryption	TKIP or AES
Group Key Update Interval	3600
RADIUS Server	
RADIUS Port	1812
RADIUS Secret	
Enable RADIUS Accounting	<input type="checkbox"/>
RADIUS Accounting Server	
RADIUS Accounting Port	1813
RADIUS Accounting Secret	
Interim Accounting Interval	600
Enable Fast Roaming (802.11k, 802.11r)	<input checked="" type="checkbox"/>

WPA2 Enterprise Authentifizierung mit WatchGuard APs

- In der WatchGuard Cloud Wi-Fi ist es ähnlich gestaltet:

The screenshot displays the configuration interface for WPA2 Enterprise authentication on a WatchGuard AP. The interface is divided into two main sections: 'TestWPA2E' and 'QNAP'.

TestWPA2E Section:

- Navigation tabs: Basic, **Security**, Network.
- Section: Select Security Level for Associations.
- Security Level: WPA2 (dropdown menu).
- Authentication Method: PSK, 802.1x.

RADIUS Settings Section:

- Buttons: PRIMARY, SECONDARY.
- Authentication Server: QNAP (dropdown menu).
- Accounting: None (dropdown menu).
- Buttons: Add/Edit (for both Authentication Server and Accounting).

QNAP Section:

- Section: QNAP.
- RADIUS Server Name: QNAP (text input).
- IP Address: 192.168.178.198 (text input).
- Authentication Port: 1812 (dropdown menu), [1-65535] (range).
- Accounting Port: 1813 (dropdown menu), [1-65535] (range).
- Shared Secret: (password input field with visibility toggle).

WPA2 Enterprise Authentifizierung mit WatchGuard APs

- *Role Based Control:*
 - Mit der rollenbasierten Steuerung können Sie den wireless Netzwerkzugriff auf autorisierte Benutzer beschränken. Benutzern wird ein kontrollierter Zugriff auf wireless Ressourcen basierend auf den ihnen zugewiesenen Rollen gewährt. Beispielsweise können Sie Benutzer auf bestimmte VLANs beschränken, Bandbreitenkontrollen anwenden, Netzwerk- und Anwendungsfirewall-Regeln erzwingen oder Benutzer basierend auf ihrem Rollenprofil auf ein Portal umleiten.

- *Vererbt von der SSID:*
 - Alle Konfigurationselemente im Rollenprofil sind auch im SSID-Profil verfügbar und gelten für Benutzer, die eine Verbindung zur SSID herstellen. Sie können die Konfigurationen für eine oder mehrere dieser Einstellungen vom SSID-Profil erben, wenn Sie keine alternative Einstellung erzwingen möchten.

Anleitungen

- WatchGuard bietet für einige Szenarien fertige Artikel an.
 1. Dynamic VLAN Assignment in WatchGuard Wi-Fi Cloud
<http://watchguardsupport.force.com/publicKB?type=KBArticle&SFDCID=kA22A000000HQJ7SAO>
 2. Authenticate Wi-Fi Cloud users with Microsoft Active Directory and NPS
https://watchguardsupport.secure.force.com/publicKB?type=Article&SFDCID=kA10H000000g36uSAA&lang=en_US

Security Hinweise

- WPA2 Enterprise ist die zurzeit sicherste Authentifizierungsmethode im Bereich Wi-Fi.
- Aber auch diese ist angreifbar, wenn man keine Zertifikate basierte Authentifizierung verwendet.
- Mit Tools wie z.B. Kali Linux oder PineApple kann der Angreifer ein Evil Twin aufbauen, welcher bei WPA2 Enterprise mit PSK den Client dazu „überredet“ beim Handshake ihn den Username und das Passwort in Klartext zu übertragen.



Live Demo



Vielen Dank!



***NOTHING GETS
PAST RED.***

