AnyConnect Samsung Knox VPN-integratiehandleiding

Inhoud

AnyConnect implementeert het Samsung Knox VPN-kader en is compatibel met de Knox VPN SDK. Het wordt aanbevolen om Knox versie 2.2 en hoger te gebruiken met AnyConnect. Alle bewerkingen van IKnoxVPNService worden ondersteund. Raadpleeg de documentatie bij IIKnoxVpnService die door Samsung is gepubliceerd voor een gedetailleerde beschrijving van elke bewerking.

Knox VPN JSON-profiel

Zoals vereist door het Knox VPN-kader, wordt elke VPN-configuratie gemaakt met behulp van een JSON-object. Dit object bevat drie belangrijke delen van de configuratie:

1. Algemene eigenschappen - "profile_attribuut"
2. Kenmerken verkoper (AnyConnect) - "verkoper"
3. Kenmerken Knox specifiek profiel - "knox"

Ondersteunde velden profiel_type

- profielnaam - unieke naam voor het aansluitingsbericht dat wordt weergegeven in de verbindingslijst van het AnyConnect-startscherm en het veld Description van het AnyConnect-aansluitingsbericht. We raden aan om maximaal 24 tekens te gebruiken om er zeker van te zijn dat deze in de verbindingslijst passen. Gebruik letters, cijfers of symbolen op het toetsenbord die op het apparaat worden weergegeven wanneer u tekst in een veld invoert. De letters zijn hoofdlettergevoelig.

- VPN_type - Het VPN-protocol dat voor deze verbinding wordt gebruikt. Geldige waarden zijn: sslipsec
- vpn_route_type - Geldige waarden zijn: 0 - System VPN1 - Per-app VPN

Raadpleeg de Samsung KNOX Framework Vendor Integration Guide voor meer informatie over de gemeenschappelijke profieleigenschappen.

AnyConnect-specifieke configuratie wordt gespecificeerd via de toets "**AnyConnectVPN**-verbinding" **in** het "kraakpand"-gedeelte. Steekproef:

```
{
"KNOX_VPN_PARAMETERS": {
"profile_attribute": {
"profileName": "SSL VPN",
"vpn_type": "ssl",
"vpn_route_type": 0
},
"vendor": {
"AnyConnectVPNConnection": {
"host": "vpn.company.com"
}
}
```

```
}
}
```

Ondersteunde AnyConnect-verbindingsvelden

- host - De domeinnaam, IP-adres of Group-URL van de ASA waarmee u verbinding kunt maken. AnyConnect voegt de waarde van deze parameter in het veld Adres van de server van het AnyConnect-verbindingsstuk in.

- Verificatie - (optioneel) Alleen van toepassing wanneer vpn_type (in profile_attributes) is ingesteld op "ipsec". Specificeert de authenticatiemethode die gebruikt wordt voor een IPsec VPN-verbinding met waarden die geldig zijn:
  EAP-AnyConnect (standaardwaarde)EAP-GTCEAP MD5EAP-MSCHAPv2IKE-PSKIKE-RSAIKE-ECDSA
- Zoals-identiteit - alleen gebruikt als de authenticatie is ingesteld op EAP-GTC, EAP-MD5 of EAP-MSCAPv2. Verstrekt de IKE-identiteit voor deze authenticatiemethoden.

- gebruikersgroep (optioneel) Het verbindingsprofiel (tunnelgroep) te gebruiken bij verbinding met de gespecificeerde host. Indien aanwezig, gebruikt in combinatie met HostAddress om een op groep gebaseerde URL te vormen. Als u het Primaire Protocol als IPsec specificeert, moet de gebruikersgroep de exacte naam van het verbindingsprofiel (tunnelgroep) zijn. Voor SSL is de gebruikersgroep de groep-URL of groep-alias van het verbindingsprofiel.

- certalias (facultatief)- Keychain alias van een client certificaat dat moet worden ingevoerd uit Android Keychain. De gebruiker moet een Android-systeemherinnering kennen voordat de cert door AnyConnect kan worden gebruikt.

- ccomcertalias (facultatief)- TIMA alias van een client certificaat dat moet worden ingevoerd uit de TIMA-certificaatwinkel. Geen actie van de gebruiker is nodig om de cert te ontvangen. Let op: Dit certificaat moet expliciet zijn gefloten, bestemd voor gebruik door AnyConnect (bv. gebruik van de Knox certificaatapplicatie).

Metagegevens over inline VPN-pakketapp

Inline app-metagegevens voor VPN-pakketten zijn een exclusieve functie die beschikbaar is op Samsung Knox-apparaten. Het wordt geactiveerd door MDM en biedt AnyConnect met de brontoepassingscontext voor het afdwingen van routing en filtering beleid. Het is vereist voor het uitvoeren van bepaalde per-app VPN-filterbeleid van de VPN-gateway op Android-apparaten. Het beleid wordt gedefinieerd om specifieke applicatie of groepen apps te lokaliseren via wildcarding en het wordt aangepast aan de bronapplicatie van elk uitgaand pakketje.

MDM-dashboard dient beheerders van een optie te voorzien om inline pakketvastlegging met metagegevens mogelijk te maken. Maar MDM kon deze optie toch hardcoderen om altijd aan te zetten voor AnyConnect, dat er gebruik van zal maken volgens het eindbeleid.

Raadpleeg het gedeelte "Een VPN-beleid per app definiëren voor Android-apparaten" in de Cisco AnyConnect Secure Mobility Client Administrator-gids voor ABBYY FineReader definiëren voor meer informatie over het beleid van AnyConnect.

MDM-configuratie

Stel "uidpid_search_enabled" in op 1 in de Knox-specifieke eigenschap voor een configuratie om inline pakketmetadata in te schakelen. Steekproef:

```
{
"KNOX_VPN_PARAMETERS": {
"profile_attribute": {
"profileName": "ac_knox_profile",
"vpn_type": "ssl",
"vpn_route_type": 1
},
"vendor": {
"AnyConnectVPNConnection": {
"host": "asa.acme.net"
}
},
"knox": {
"uidpid_search_enabled": 1
}
}
}
```