Guida all'integrazione di AnyConnect VPN Knox VPN MDM

Sommario

AnyConnect implementa il framework VPN Samsung Knox ed è compatibile con Knox VPN SDK. Si consiglia di usare Knox versione 2.2 e successive con AnyConnect. Sono supportate tutte le operazioni da IKnoxVpnService. Per una descrizione dettagliata di ciascuna operazione, vedere la documentazione IKnoxVpnService pubblicata da Samsung.

Profilo JSON Knox VPN

Come richiesto dal framework VPN Knox, ogni configurazione VPN viene creata utilizzando un oggetto JSON. Questo oggetto contiene tre sezioni principali della configurazione:

1. Attributi generali - "profile_attribute"
2. Attributi specifici del fornitore (AnyConnect) - "fornitore"
3. Attributi di profilo specifici di Knox - "knox"

Campi profile_attribute supportati

- profileName: nome univoco della voce di connessione da visualizzare nell'elenco delle connessioni della schermata iniziale di AnyConnect e nel campo Description della voce di connessione AnyConnect. È consigliabile utilizzare un massimo di 24 caratteri per garantire che rientrino nell'elenco delle connessioni. Utilizzare lettere, numeri o simboli sulla tastiera visualizzata sul dispositivo quando si immette del testo in un campo. Le lettere fanno distinzione tra maiuscole e minuscole.

- vpn_type: il protocollo VPN utilizzato per questa connessione. I valori validi sono: SSLipsec
- vpn_route_type: i valori validi sono: 0 - VPN di sistema1 - VPN per app

Per ulteriori informazioni sugli attributi comuni del profilo, vedere la Guida all'integrazione dei fornitori di Samsung KNOX Framework.

La configurazione specifica di AnyConnect è specificata tramite la chiave "**AnyConnectVPNConnection**" all'interno della sezione "fornitore". Esempio:

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

Campi AnyConnectVPNConnection supportati

- host: nome di dominio, indirizzo IP o URL di gruppo dell'appliance ASA con cui connettersi. AnyConnect inserisce il valore di questo parametro nel campo Server Address della voce di connessione AnyConnect.

- authentication - (optional) Applicabile solo quando vpn_type (in profile_attributes) è impostato su "ipsec". Specifica il metodo di autenticazione utilizzato per una connessione VPN IPSec. I valori validi sono:
  EAP-AnyConnect (valore predefinito)EAP-GTCEAP-MD5EAP-MSCHAPv2IKE-PSKIKE-RSAIKE-ECDSA
- ike-identity: utilizzato solo se l'autenticazione è impostata su EAP-GTC, EAP-MD5 o EAP-MSCAPv2. Fornisce l'identità IKE per questi metodi di autenticazione.

- usergroup (facoltativo) Il profilo di connessione (gruppo di tunnel) da utilizzare per la connessione all'host specificato. Se presente, utilizzata in combinazione con HostAddress per formare un URL basato su gruppo. Se si specifica IPsec come protocollo primario, il gruppo di utenti deve essere il nome esatto del profilo di connessione (gruppo di tunnel). Per SSL, il gruppo utenti è l'URL o l'alias del gruppo del profilo di connessione.

- certalias (facoltativo): alias KeyChain di un certificato client che deve essere importato da Android KeyChain. L'utente deve confermare la ricezione di una richiesta di sistema Android prima che il certificato possa essere utilizzato da AnyConnect.

- ccmcertalias (facoltativo): alias TIMA di un certificato client da importare dall'archivio certificati TIMA. Per ricevere il certificato, non è necessaria alcuna azione da parte dell'utente. Nota: il certificato deve essere stato esplicitamente autorizzato per l'uso da parte di AnyConnect (ad esempio, usando l'API CertificatePolicy di Knox).

Metadati app pacchetti VPN inline

I metadati delle app in linea per i pacchetti VPN sono una funzionalità esclusiva disponibile sui dispositivi Samsung Knox. È abilitato da MDM e fornisce ad AnyConnect il contesto dell'applicazione di origine per applicare i criteri di routing e filtro. È necessario per implementare alcuni criteri di filtro VPN per app dal gateway VPN sui dispositivi Android. I criteri vengono definiti per individuare specifici ID applicazione o gruppi di applicazioni tramite caratteri jolly e vengono confrontati con l'ID applicazione di origine di ciascun pacchetto in uscita.

Il dashboard MDM deve fornire agli amministratori un'opzione per abilitare i metadati dei pacchetti in linea. In alternativa, MDM può hardcode questa opzione in modo che sia sempre abilitata per AnyConnect, che la utilizzerà in base ai criteri headend.

Per ulteriori informazioni sui criteri VPN per app di AnyConnect, vedere la sezione "Define a Per App VPN Policy for Android Devices" nel manuale Cisco AnyConnect Secure Mobility Client Administrator Guide.

Configurazione MDM

Per abilitare i metadati del pacchetto in linea, impostare "uidpid_search_enabled" su 1 nell'attributo specifico Knox per una configurazione. Esempio:

```
{
"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
}
}
}
```