



Communauté Cisco Télétravail, Collaboration & RaVPN. Intégration

Sécurité, Collaboration

Alain Faure

Chef de projet d'Infrastructures Informatiques | CCIE R&S # 8935

4 mai 2021

Introduction

Les experts de la Communauté Cisco

Alain Faure

Chef de projet
d'Infrastructures Informatiques
CCIE R&S # 8935



Présentateur

Merci d'être avec
nous aujourd'hui !

Téléchargez la présentation sur

<https://bit.ly/WEBsld-may21>



Participez avec nous et posez des questions

La présentation comprendra aussi quelques questions du public.
Nous vous invitons cordialement à participer activement aux questions que vous pourrez poser pendant cette séance sur le panneau à droite « Q&R ».

Résolvez vos doutes et partagez votre opinion



Ordre du jour



Présentation



Architecture



MEO - Infrastructure



MEO - AnyConnect



MEO - Collaboration

1

Présentation

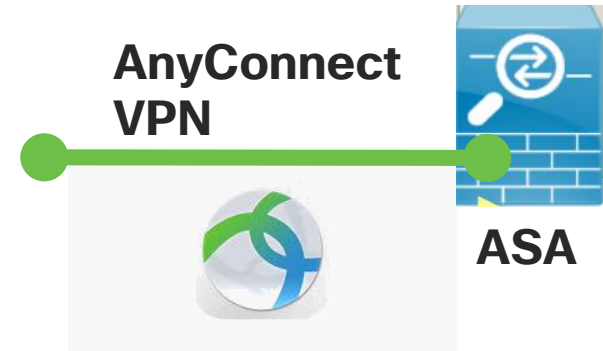
Introduction (1)

Télétravail: Accès distant comme **composant central** de l'architecture IT. Le **VPN (Virtual Private Network)** est le support de communication.

Il existe différents types de **VPN** chez Cisco :

- IPSec VPN
- Site to site VPN
- **AnyConnect VPN**
- Clientless VPN (WebVPN)

Concentrateur de VPN Cisco -Ex: Routeur IOS, **ASA**-



Introduction (2)

Comme d'habitude, je vous propose ici une vision globale, puis une plongée dans les détails techniques de la mise en œuvre (MEO). Il y a beaucoup de configuration : **ASA, IOS, CUCM**. Et aussi beaucoup de référence à la documentation, qui je pense est une richesse qui distingue Cisco des autres constructeurs.

Nous allons nous attarder sur **AnyConnect VPN**, puisque c'est la solution proposée par Cisco pour connecter les clients distants.

RAVPN : Remote Access VPN



Les RFCs, normes et comportements à connaître

L'interopérabilité en terme de VPN est assez liée au constructeur. Il est préférable d'avoir une chaîne de bout en bout cohérente (du même éditeur).

IEEE 802.1X, IEEE 802.1AE

Lire aussi wikipédia : <https://fr.wikipedia.org/wiki/IPsec> il y a plein de RFC qui couvrent les aspects de sécurisations des échanges sur Internet.



Références de documentation - ASA

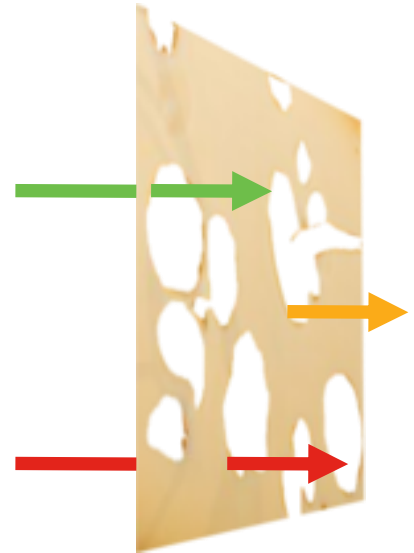
« AnyConnect Implementation and Performance/Scaling Reference for COVID-19 Preparation »

« Remote Access VPN Design Guide - **ASA** Security Business Group Network Security Technical Marketing Engineering 09 July 2020 »

ASA : Adaptive Security Appliance (*historiquement un firewall*)

Une inspiration pour la partie Collaboration :

« Voice and Video Enabled IPSec VPN (V 3 PN) Solution Reference Network Design January 2004 »





2

Architecture

CISCO AnyConnect– Way more than VPN

VPN Features

Basic
VPN



Advanced
VPN



Endpoint
Compliance



Inspection
Service



Enterprise
Access



Threat
Protection



Network
Visibility



Roaming
Protection



CISCO AnyConnect

Integration with other Cisco solutions



ISR



ASR/CSR



Adaptive
Security
Appliance
(ASA)



Identity
Services
Engine
(ISE)



Cloud Web
Security
Services
(CWS+ WSA)



Switches
and
Wireless
Controllers



Advanced
Malware
Protection

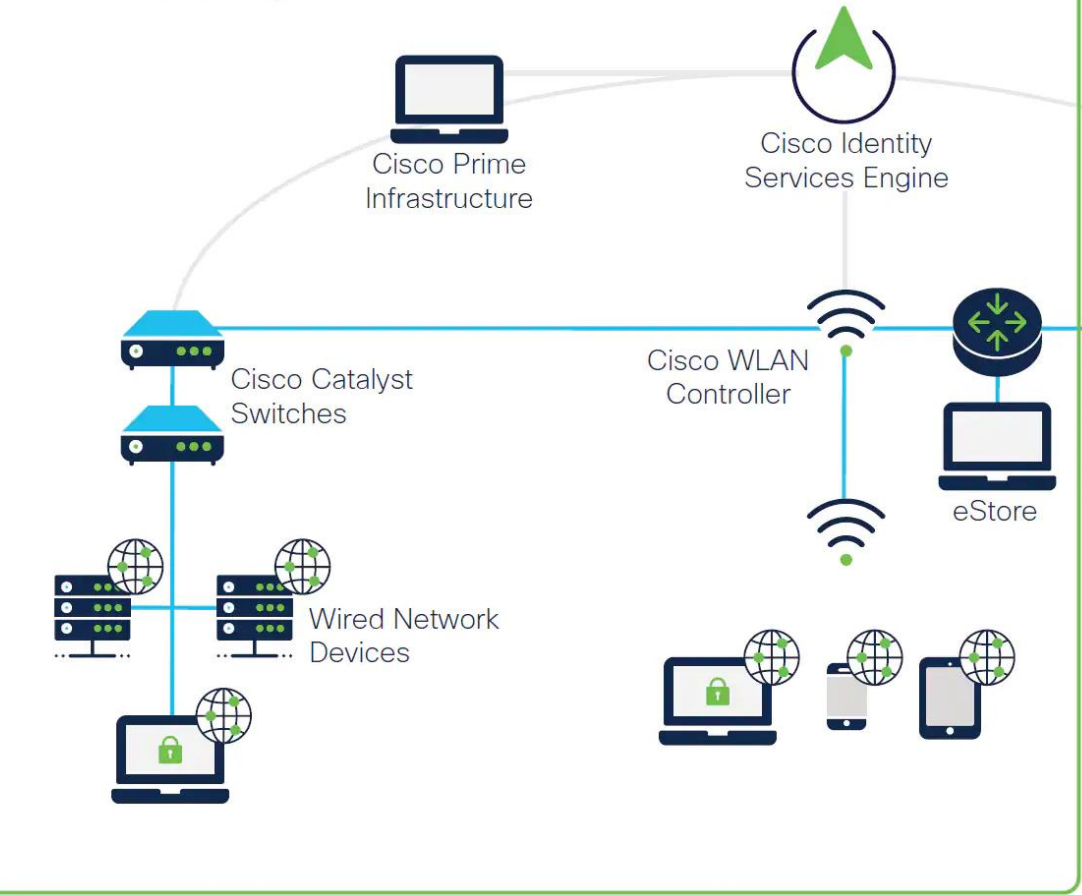


Netflow
collectors

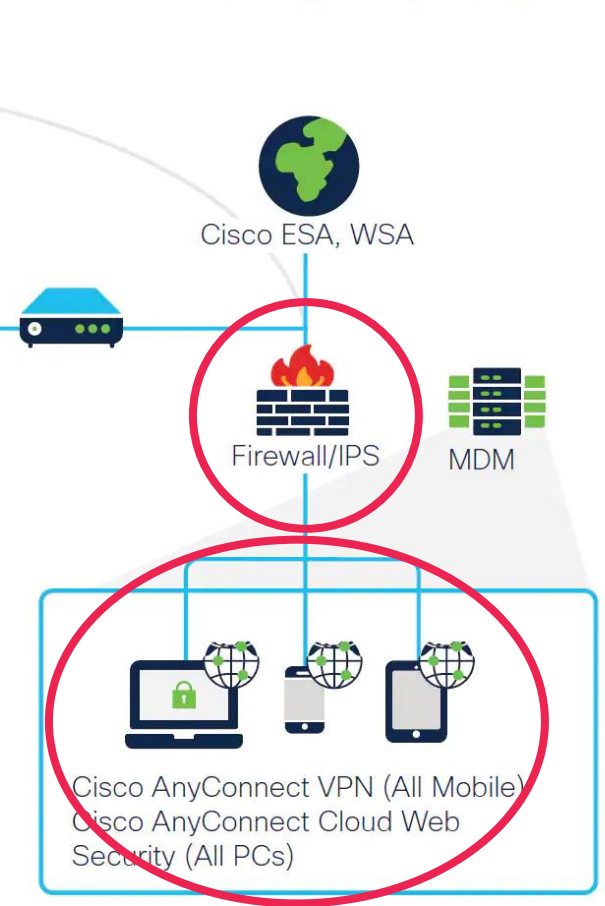


Umbrella
Services

Inside the Enterprise



Outside the Enterprise (BYOD)



Choix du cœur ASA vs FTD

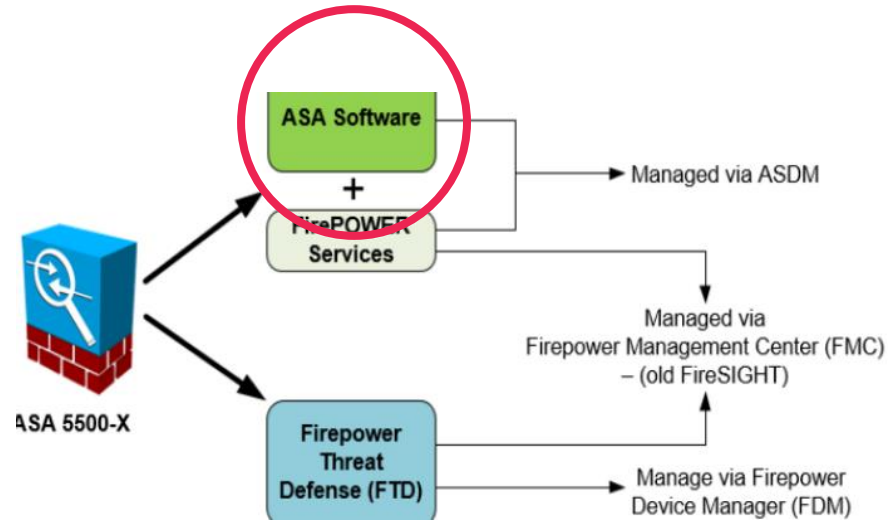
Point de convergence des VPNs:

ASA+FirePower services est équivalent à FTD)

FTD (Firepower Thread Defence)

Base matérielle :

ASA 5500-x (plus de fonctionnalité, plus de performances)



Choix du Matériel

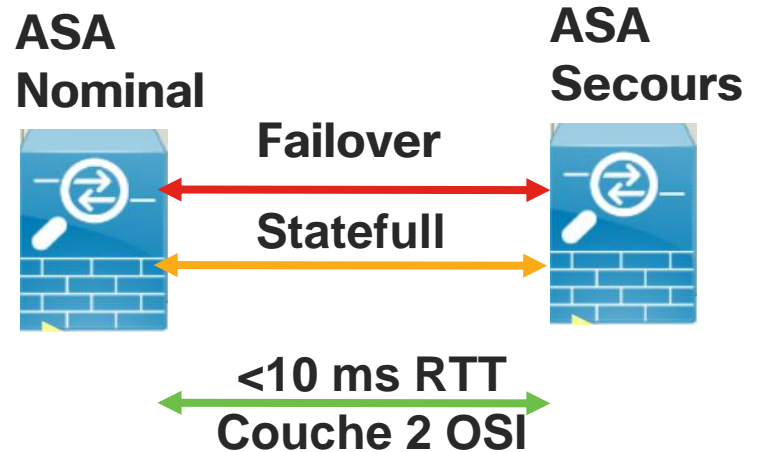
Selon le nombre de sessions supportées simultanément :

FP1010:75 ; FP1140:400

ASA5545 : 2500

(Remote Access VPN Design Guide - ASA 09/07/2020)

Il est préférable d'avoir 2 ASA pour l'architecture nominal / secours.



3 types de licences client AnyConnect

AnyConnect Plus

AnyConnect Apex (AnyConnect Plus
+ fonctionnalités supplémentaires)

AnyConnect VPN only

Voir « Cisco AnyConnect Ordering
Guide »

Pour voir les licences courantes

Show version



```
Licensed features for this platform:
Maximum Physical Interfaces      : Unlimited
Maximum VLANs                   : 150
Inside Hosts                     : Unlimited
Failover                         : Active/Active
VPN-DES                          : Enabled
VPN-3DES-AES                     : Enabled
Security Contexts               : 2
GTP/GPRS                        : Disabled
SSL VPN Peers                   : 2
Total VPN Peers                 : 750
Shared License                   : Disabled
AnyConnect for Mobile           : Disabled
AnyConnect for Cisco VPN Phone  : Disabled
AnyConnect Essentials           : Disabled
Advanced Endpoint Assessment    : Disabled
UC Phone Proxy Sessions         : 2
Total UC Proxy Sessions         : 2
Botnet Traffic Filter           : Disabled
```

3 Types de protocole utilisés

- **TLS** -Transport Layer Security-(TCP 443) meilleur choix TLS 1.2 (*pour SSL VPN*)
- **DTLS** (UDP 443) faible temps de latence (Voix, Vidéo).
Implémentation Cisco de DTLS (RFC 6347)
- **IKEv2** (Echange des clés)

Choix d'identification Multi-facteurs

- ASA SSL VPN / **SAML** (Protocole basé sur XML)
- ASA SSL VPN / **RADIUS**
- ASA SSL VPN / **LDAPS**

Choix de robustesse

- Serveur de secours
- Haute disponibilité Actif/Passif
- Partage de charge pour VPN natifs avec load balancer externe
- Partage de charge pour DNS



Le Monitoring

Particulièrement important dans un contexte de production à distance, l'utilisateur ayant besoin d'un support rapide, efficace et pro-actif :

- VPN dashboard
- Logging avec Syslog
- SNMP
- CLI Monitoring
- Cisco Endpoint Security Analytics



Recommandations

Dynamic split tunneling : Pour isoler le trafic Internet du trafic de l'entreprise.

QoS : Pour garantir la Qualité de Service aux applications Voix, vidéo et de collaboration.

Temps : Veillez à ce que tous les équipements soient à la bonne heure (protocole **NTP**)

Designer l'architecture la plus robuste possible. Mm géographiquement

(Perte du concentrateur VPN=perte de production importante)



Les Clients

AnyConnect peut s'installer sur beaucoup de plateformes : **Linux, Windows, MacOS Apple, Android, iOS (Apple)** etc.

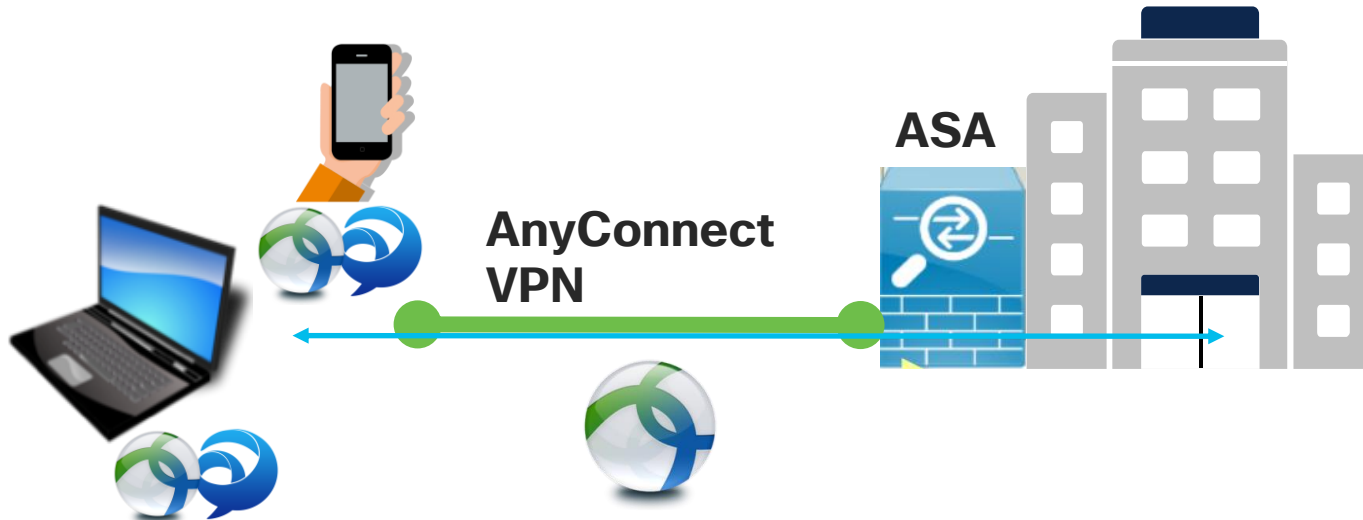
Mais AnyConnect peut être un moyen de connecter des **IP Phones Cisco...**

ou des clients **JABBER.**



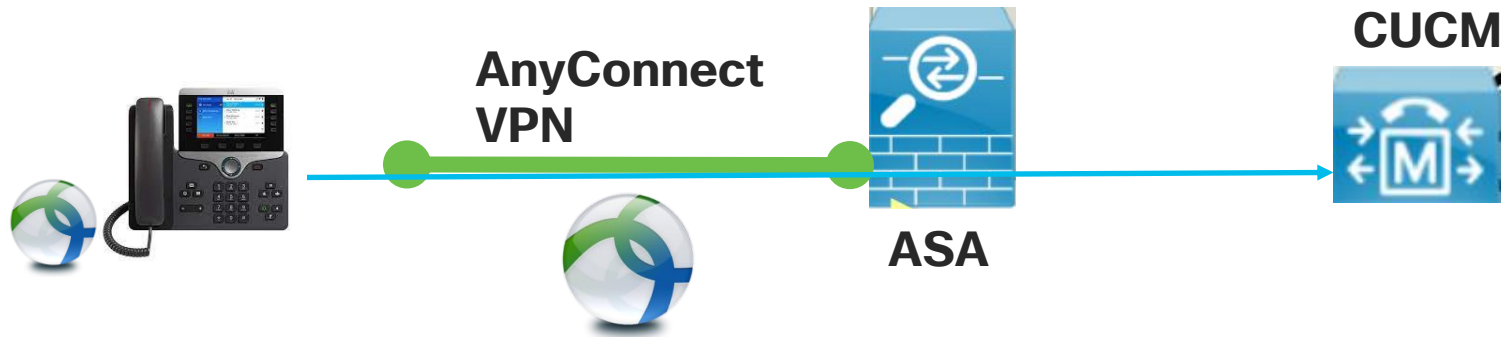
AnyConnect VPN

- ASA
- Client AnyConnect Cisco sur Linux



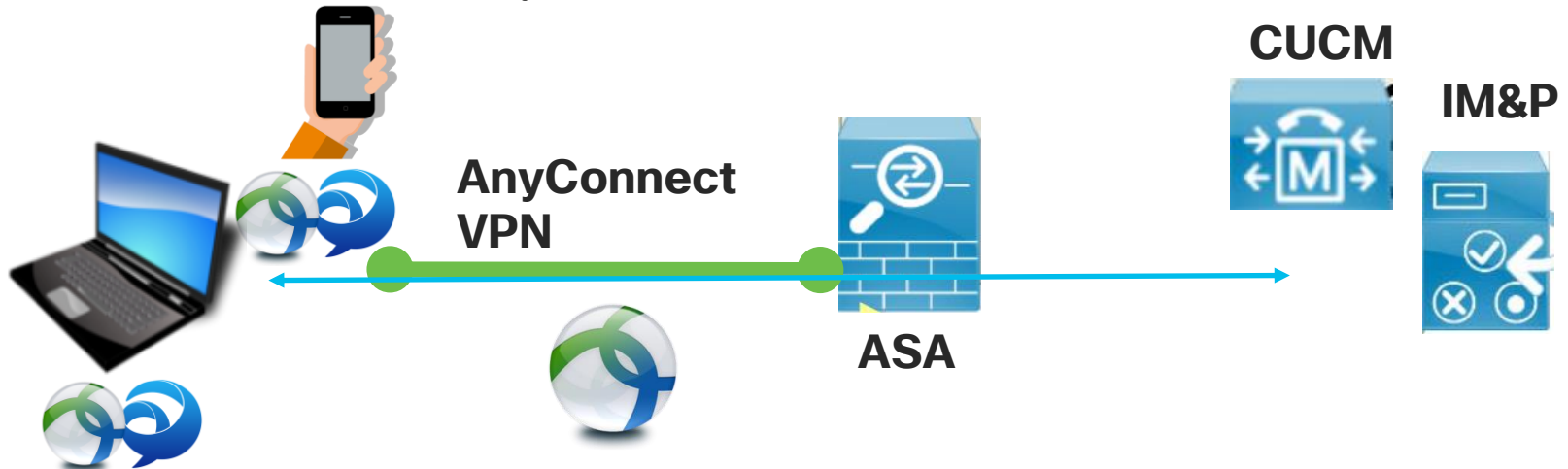
Intégration IP Phone Cisco CUCM ASA

- CUCM ou CME
- ASA ou Routeur IOS
- IP Phone VPN Cisco



Intégration Jabber CUCM ASA

- CUCM
- ASA
- Jabber et client Any Connect Cisco



Quel est le type de VPN Cisco le plus adapté à un télétravailleur ?

Polling Question - Sondage 1

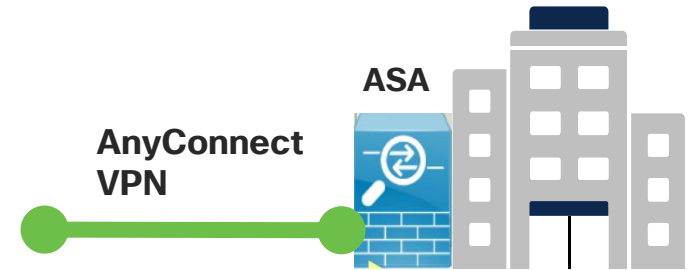
- A. IPSec VPN
- B. AnyConnect VPN
- C. V³PN



3

MEO - Infrastructure

Implémentation sur ASA



Protocoles

Configuration en mode CLI

(demande de travailler aussi sur des fichiers XML pour les profils).

- DTLS est optionnel, peu désescalader en TLS si nécessaire
- un tunnel TLS est maintenu en parallèle à DTLS pour les **keepalives** (PMTU discovery) et le **mode secours** (backup).
- Un firewall entre AnyConnect et ASA doit permettre le passage de **TCP 443** et **UDP 443** pour que **DTLS** fonctionne

Certificats

Les clients doivent faire confiance aux certificats ASA, au choix :

Autorités publiques de Certification (bien connus)

-Ex : Verisign, Let's Encrypt-

Autorité de certificat d'entreprise

-Ex : Microsoft Active Directory-

« **Self-Signed** » (certificat importé sur chaque client)

Le FQDN doit être dans le champ « Subject » du certificat

Mode nominal / Secours

Facile: Utilise le mécanisme de l'ASA :

- Apparaît comme un ASA partageant les adresses IP et MAC
- Changements de configuration répliqués (avec certificats)

Ne sont pas répliqués : AnyConnect Images, AnyConnect Profiles.

- VPN sessions répliqués : bascule sans impact
- Nécessite une connectivité couche 2 entre les ASA

Configuration ASA (Phasing)

- Configuration de l'ASA pour un déploiement Web du Client
- Autoriser l'installation permanente du client
- Configuration du protocole DTLS
- Connexion des utilisateurs distants
- Autoriser le téléchargement des Client Profile AnyConnect
- Autoriser les fonctionnalités additionnelles des Client Profile AnyConnect
- Autoriser le démarrage avant le Logon
- Traductions pour les messages utilisateur AnyConnect
- Configuration des fonctionnalités avancées AnyConnect SSL
- Surveillance AnyConnect

Configuration de l'ASA pour un déploiement Web du Client (1)

Principe : On définit : « les connexions profil » qui indiquent les caractéristiques du tunnel VPN.

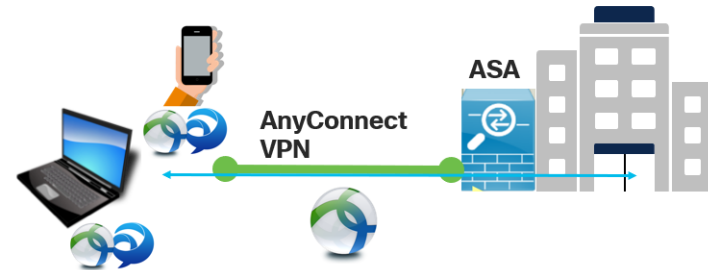
```
tunnel-group teletravailleurs
```

On définit : Les politiques de groupe « Group policies »

```
group-policy marketing
```

On définit : Les valeurs pour les utilisateurs « Users ».

```
username gege password simpl3 encrypted privilege 12
```



Configuration de l'ASA pour un déploiement Web du Client (2)

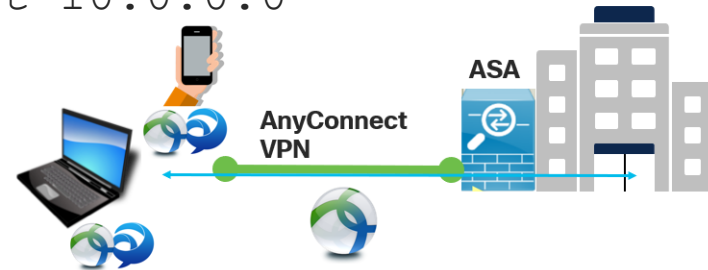
```
webvpn
enable outside
anyconnect image anyconnect-linux-2.3.0254-k9.pkg 3
anyconnect enable
tunnel-group-list enable

ip local pool vpn_address 209.165.200.225-209.165.200.254
Mask 255.255.255.224

access-list split_range standard permit 10.0.0.0
255.255.255.0
```

Téléch. par TFTP

Ordre



Configuration de l'ASA pour un déploiement Web du Client (3)

Attributs de connexion, selon :

- URL
- Choix du groupe par utilisateur
- Certificat prè-chargé dans le client



L'utilisateur appartient à
marketing

```
group-policy marketing internal  
group-policy marketing attributes  
  dns-server value 8.8.8.8  
  vpn-tunnel-protocol ssl-client ssl-clientless  
  split-tunnel-policy tunnelspecified  
  split-tunnel-network-list value split_range  
  default-domain value fromage.com
```

Configuration de l'ASA pour un déploiement Web du Client (4)

```
tunnel-group teletravailleurs type remote-access  
tunnel-group teletravailleurs general-attributes  
  address-pool vpn_address  
  default-group-policy marketing
```

```
tunnel-group teletravailleurs general-attributes  
  authentication certificate  
  group-alias teletravailleurs enable
```

Dévalider l'installation permanente du client

Par défaut le client n'est pas désinstallé après une fin de communication.

Pour forcer la désinstallation :

```
group-policy marketing attributes
```

```
anyconnect keep-installer installer none
```

Configuration du DTLS

Par défaut DTLS est autorisé quand l'accès SSL VPN est autorisé sur une interface. Si DTLS est dévalidé les connexions SSL VPN se connectent seulement avec un tunnel SSL VPN. Pour cela Dead Peer Detection (DPD) doit être validé.

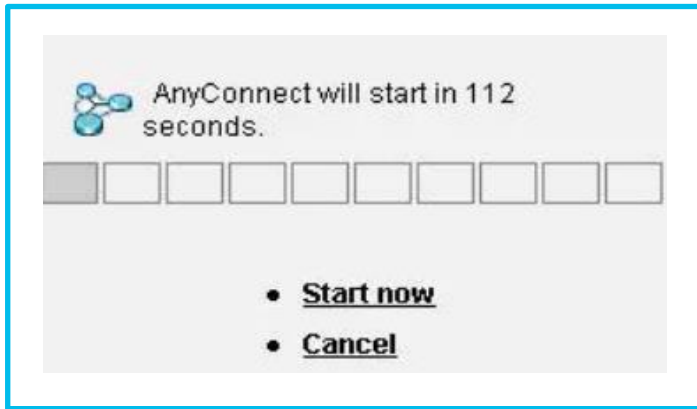
```
enable outside  
port 555  
dtls port 556
```

```
group-policy marketing attributes  
anyconnect ssl dtls enable  
anyconnect dtls compress lzs
```

Connexion des utilisateurs distants

Il est possible pour l'ASA de demander à l'utilisateur distant s'il veut télécharger le client.

```
anyconnect ask enable default anyconnect timeout 10
```



Secondes
avant action
par défaut

Autoriser les téléch. des profils (1)

```
anyconnect profiles marketing disk0:/marketing_hosts.xml
anyconnect profiles engineering disk0:/engineering_hosts.xml
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/">
<ServerList>
<HostEntry>
<HostName>SuperOrdinateur</HostName>
<HostAddress>SuperOrdinateur.Boite.com</HostAddress>
</HostEntry>
</ServerList>
<ServerList>
<HostEntry>
<HostName>MyGuest</HostName>
<HostAddress>guest.Vendeur01.com</HostAddress>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```



Editer avec
ASDM/ISE

Autoriser les téléch. des profiles (2)

```
dir cache:/stc/profiles
```

```
Directory of cache:stc/profiles/
```

```
0      ----  774          10:13:39 Mar 22 2021  engineering.xml
0      ----  774          11:08:20 Mar 22 2021  marketing.xml
```

```
2426592 bytes total (18214581 bytes free)
```

```
anyconnect profiles value marketing type vpn
```

Autoriser la mise à jour différée du client

Autorise la boîte de dialogue pour l'utilisateur

```
anyconnect-custom-attr DeferredUpdateAllowed description  
"Indicates if the deferred update feature is enabled or not"  
anyconnect-custom-attr DeferredUpdateDismissTimeout
```

```
group-policy marketing attributes
```

```
webvpn
```

```
anyconnect-custom DeferredUpdateDismissTimeout value 10  
anyconnect-custom DeferredUpdateAllowed value true
```

Autoriser la conservation de DSCP

```
anyconnect-custom-attr DSCPPreservationAllowed description  
Set to control Differentiated Services Code Point (DSCP) on  
Windows or OS X platforms for DTLS connections only.
```

```
anyconnect-custom-data DSCPPreservationAllowed true
```

Autoriser des fonctionnalités Additionnelles

```
[no] anyconnect modules {none | value string}
```

Traduction des messages pour les utilisateurs

Un peu long pour être traité ici, se reporter au document :
« CLI Book 3: Cisco ASA Series VPN CLI Configuration Guide »
Chapter: « AnyConnect VPN Client Connections »
→ Translating Languages for AnyConnect User Messages

```
show import webvpn translation-table
```

```
export webvpn translation-table AnyConnect  
template tftp://209.165.200.225/client
```

```
import webvpn translation-table AnyConnect  
language es-us tftp://209.165.200.225/client
```

Configuration des fonctionnalités avancées

Configure Dead Peer Detection

```
group-policy marketing attributes
```

```
anyconnect dpd-interval gateway 30
```

```
anyconnect dpd-interval client 10
```

Adjust MTU Size (de 576 à 1406 octets) pour SSL VPN

```
group-policy marketing attributes
```

```
anyconnect mtu 1200
```

Surveillance anyConnect

```
show vpn-sessiondb
```

```
show vpn-sessiondb anyconnect
```

Terminer une session :

```
vpn-sessiondb logoff name user01
```


Quel est le protocole de chiffrement le plus complexe à décrypter ?

Polling Question - Sondage 2

- A. AES
- B. DES
- C. 3DES

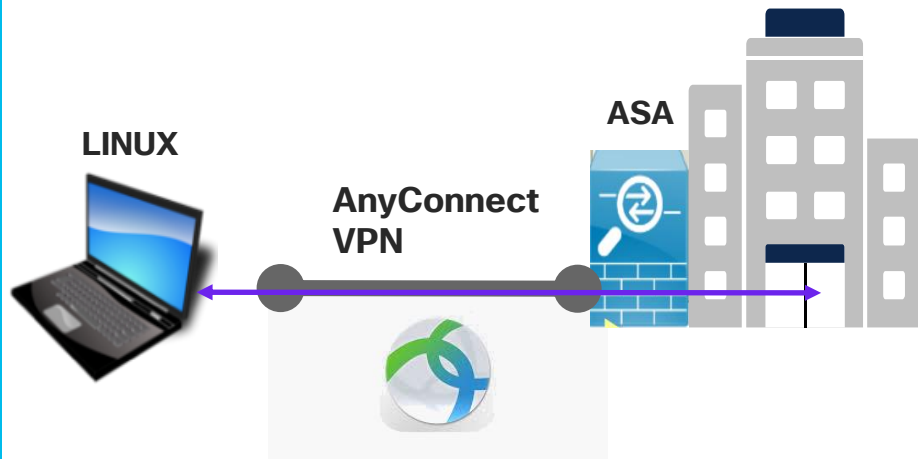


4

MEO – Any Connect VPN

Architecture
simple:

AnyConnect, ASA
et Linux



Client sur Linux

Document original :

Configure **AnyConnect** Secure Mobility Client for **Linux** using Client Certificate Authentication on an **ASA**
(voir [cisco.com](https://www.cisco.com))

Installation du client sur Linux

```
tar -xvf anyconnect-linux64-4.6.03049-predeploy-k9.tar.gz  
cd anyconnect-linux64-4.6.03049/vpn/  
./vpn_install.sh
```

Création du certificat sur Linux

```
openssl genrsa -des3 -out server.key 2048  
openssl rsa -in server.key -out server.key.insecure  
mv server.key server.key.secure  
mv server.key.insecure server.key
```

```
openssl req -new -key server.key -out server.csr
```

```
cat server.csr
```

➤ donne le CSR (Certificate Signing Request)

Faire une requête au CA (Certificate Authority) pour avoir un certificat d'identité utilisateur.

Mise en place du certificat CA sur Linux

Créer un fichier .pem dans “/home/utilisateur/.cisco/certificates/client”
touch myclient.pem

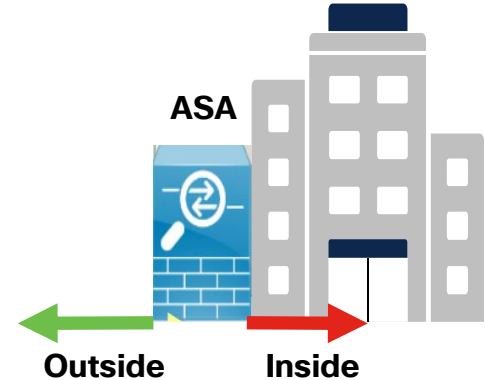
Copier le certificat (Base64) remis par le CA dans le fichier .pem

Placer ce certificat dans le répertoire *opt/.cisco/certificates/ca*

Configuration ASA - interfaces / routage

```
interface GigabitEthernet0/1
nameif outside
security-level 0
ip address 10.0.0.1 255.255.255.0
!
interface GigabitEthernet0/2
nameif inside
security-level 100
ip address 20.0.0.1 255.255.255.0

asdm image disk0:/asdm-791.bin
route outside 0.0.0.0 0.0.0.0 10.0.0.2 1
```



Configuration ASA – addresses clients / ACL

```
ip local pool vpn_address 192.168.3.2-192.168.3.254 mask  
255.255.255.0
```

```
access-list split_range standard permit 20.0.0.0  
255.255.255.0
```


Configuration ASA – Trustpoint ASA ID Certif.

```
crypto ca trustpoint IDENTITY
enrollment terminal
subject-name CN=anyconnect.fromage.com
keypair ID_CERT
crl configure

ssl trust-point IDENTITY outside
```

Configuration ASA - Anyconnect

```
webvpn
enable outside
anyconnect image disk0:/anyconnect-linux64-4.6.03049-
webdeploy-k9.pkg 1
anyconnect enable
tunnel-group-list enable
```

Configuration de l'ASA pour un déploiement Web du Client (3)

Attributs de connexion, selon :

- URL
- Choix du groupe par utilisateur
- Certificat prè-chargé dans le client



L'utilisateur appartient à
marketing

```
group-policy marketing internal  
group-policy marketing attributes  
  dns-server value 8.8.8.8  
  vpn-tunnel-protocol ssl-client ssl-clientless  
  split-tunnel-policy tunnelspecified  
  split-tunnel-network-list value split_range  
  default-domain value fromage.com
```

Configuration de l'ASA pour un déploiement Web du Client (4)

```
tunnel-group teletravailleurs type remote-access  
tunnel-group teletravailleurs general-attributes  
  address-pool vpn_address  
  default-group-policy marketing
```

```
tunnel-group teletravailleurs general-attributes  
  authentication certificate  
  group-alias teletravailleurs enable
```

Certificats (1) – Peuvent être générés sur ASA

Génère un certificat auto-signé avec CLI sur ASA

1) Création de la paire de clés RSA:

```
crypto key generate rsa label SSL-Key modulus 1024 noconfirm
```

2) Création d'un trust-point

```
crypto ca trustpoint  
SSL-trustpoint
```

```
subject-name CN=adresse_IP_ASA (ou FQDN)
```

```
keypair SSL-Key
```

```
fqdn none
```

```
enrollment terminal
```

!

```
crypto ca enroll SSL-trustpoint noconfirm
```

Command	Purpose
crypto key zeroize rsa	Removes key pairs.
hostname(config)# crypto key zeroize rsa	

Certificats (2)

Entrée « Yes » et <Enter>

```
Display Certificate Request to terminal? [yes/no]: yes
```

This generates your CSR:

```
~CSR~ ← CSR : Certificate
```

Copier le CSR et envoyez-le à votre autorité de certificat.

Quels IP Phone Cisco supportent le VPN ?

Polling Question - Sondage 4

- A. 8900
- B. 7861
- C. 9971



5

MEO – Collaboration

Le sujet

Le transit de **la Voix et de la Vidéo** à travers un VPN ou un tunnel n'est pas anodin :

- Ralentissement de la vitesse de propagation
- Multiplication des points de rupture de QoS

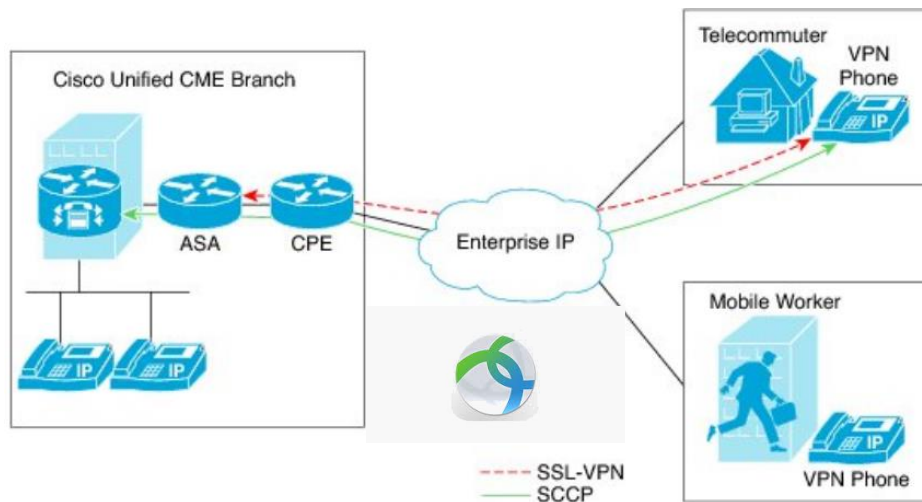
Voir le SRND « Chapter 2 V3PN Solution Overview and Best Practices – General Best Practices Guidelines » pour des recommandations pour le trafic VoIP et Vidéo.



Architecture avec CME sur IOS et ASA

(Cf. Cisco Unified Communications
Manager Express System
Administrator Guide - SSL VPN
Client for SCCP IP Phones)

Voici une architecture basée sur
un routeur avec CME et ASA
comme point de concentration de
VPN pour des téléphones IP
PHONE SCCP.



Sur IOS CME 14

Références :

« Cisco Unified Communications Manager Express Command Reference » pour version 14

« Cisco Unified Communications Manager Express System Administrator Guide » Last Modified: 2021-04-09

Prérequis

- CME 8.5 minimum
- Securityk9 licence pour ISR-G2 + NTP joignable !
- IP Phone SCCP 79xx
- ASA5500
- Package anyconnect-winxxx.pkg
- ASA licences (AnyConnect for Cisco VPN Phone)

IOS CME 14 – Configuration IP PBX IOS

Voir le document pour la
procédure exacte.

```
telephony-service
max-ephones 10
max-dn 20
ip source-address 10.0.0.1
port 2000
cnf-file

load [phone-type firmware-
file]
```

```
ephone-dn 3
number 3000
```

```
ephone 3
description 3000
mac-address 112233445566
type 7942
button 1:3
```

```
telephony-service
create cnf-files
reset all
```

IOS CME 14 – Configuration CA Serveur IOS

```
crypto pki server cme_root  
  
database level complete  
database url nvram:  
grant auto  
lifetime certificate 7305  
lifetime ca-certificate 7305
```

```
Crypto pki trustpoint  
cme_cert  
  
enrollment url  
http://192.168.20.1:80  
revocation-check none
```

```
crypto pki trustpoint  
cme_root  
  
enrollment url  
http://192.168.20.1:80  
revocation-check none  
rsa-keypair cme_root
```

Trustpoint pour l' ASA

Trustpoint pour le CME

```
show crypto pki certificates  
show ephone
```

IOS CME 14 – Configuration ASA

Créer un trustpoint et obtenir le certificat du CME

```
crypto key generate rsa label cmeasa
crypto ca trustpoint asatrust
  enrollment url http://192.168.20.1:80
  subject-name cn=cmeasa.cisco.com
  crl nocheck
  keypair cmeasa
```

```
crypto ca authenticate asatrust
crypto ca enroll asatrust
```

Vérifier

```
show crypto ca certificates
```

IOS CME 14 – Configuration ASA (Suite)

Configurer les paramètres SSL

```
ssl encryption 3des-sha1 aes128-sha1 aes256-sha1 des-sha1 null-sha1
ssl trust-point asatrust
ssl trust-point asatrust inside
ssl trust-point asatrust outside
no ssl certificate-authentication interface outside port 443
ssl certificate-authentication interface inside port 443
```

Interdit le NAT par le VPN

```
access-list no_nat_to_vpn extended permit ip any 9.10.60.0 255.255.255.0
nat (inside) 0 access-list no_nat_to_vpn
```


IOS CME 14 – Configuration ASA (suite)

Config. De base

```
enable inside
enable outside
svc image disk0:/anyconnect-
win-2.4.1012-k9.pkg 1
svc enable
```

```
ip local pool SSLVPNphone_pool
192.168.20.50-192.168.20.70
mask 255.255.255.0
```

Politiques de groupe

```
group-policy SSLVPNphone internal
group-policy SSLVPNphone attribute
    banner none
    vpn-simultaneous-logins 10
    vpn-idle-timeout none
    vpn-session-timeout none
    vpn-tunnel-protocol svc webvpn
    address-pools value
        SSLVPNphone_pool
```

webvpn

```
    svc dtls enable
    svc keepalive 120
    svc ask none
```

IOS CME 14 – Configuration ASA (suite)

Config. Tunnel SSL VPN

```
tunnel-group SSLVPN_tunnel type remote-access
tunnel-group SSLVPN_tunnel general-attributes
    address-pool SSLVPNphone_pool
    default-group-policy SSLVPNphone
tunnel-group SSLVPN_tunnel webvpn-attributes
```

Webvpn

```
group-url https://9.10.60.254/SSLVPNphone enable
```

IOS CME 14 – Configuration ASA (suite)

Config. la base de données utilisateur

```
username anyone password cisco
```

```
username anyone attributes
```

```
vpn-group-policy SSLVPNphone
```

```
vpn-tunnel-protocol IPsec l2tp-ipsec svc webvpn
```

```
webvpn
```

```
svc dtls enable
```

```
svc ask none
```

Autorise le trafic média inter-ASA

```
same-security-traffic permit inter-interface
```

```
same-security-traffic permit intra-interface
```

IOS CME 14 – Configuration CME IOS

Configure le VPN Group et le Profile sur le CME

```
voice service voip
  vpn-group 1
  vpn-gateway https://9.10.60.254/SSLVPNphone
  vpn-hash-algorithm sha-1
  vpn-trustpoint 1 trustpoint cme_cert

vpn-profile 1
  host-id-check disable
```

IOS CME 14 – Configuration CME IOS

Associe le VPN Group et le Profile sur le SCCP IP Phone

```
telephony-service  
create cnf-files
```

```
ephone 3  
Vpn-group 1  
vpn-profile 1
```

```
telephony-service  
create cnf-files  
reset all
```

IOS CME 14 – Configuration du Téléphone

Settings > Network Configuration > IPv4 Configuration > Alternate TFTP
Enter the CUCME address as the alternate TFTP Server 1.

Save the phone configuration.

Verify if the VPN is enabled from the Settings > Security Configuration > VPN

When you press “Enable” from this menu, it should prompt for username and password.

Connect the phone to the network from home or a remote location

Settings > Security Settings > VPN Configurations?

Enable VPN

Enter Username and Password. Phone will register with CUCME.

Que signifie la terminaison de fichier « .pem » ?

Polling Question - Sondage 4

- A. Pre-Encrypted Mail
- B. Pre-Enabling Mail
- C. Private Encrypted Mail
- D. Private Enhanced Mail



Sur CUCM

- Terminaison VPN sur IOS
- Terminaison VPN sur ASA

Références :

« Feature Configuration Guide for Cisco Unified Communications Manager - VPN Client »



CUCM - Prérequis

Pour VPN sur Cisco IOS

IOS 15.1(2)T minimum, Feature Set/License: Universal (Data & Security & UC) for IOS ISR-G2 and ISR-G3, Advanced Security for IOS ISR

Pour VPN sur ASA

ASA software (version 8.0.4 or later) and a compatible ASDM
ASA licences (AnyConnect for Cisco VPN Phone)

CUCM – Configuration IOS

CUCM : Générer et enregistrer le certificat CAPF pour authentifier le téléphone IP avec un LSC.

CUCM OS Administration / Security / Certificate Management
Cisco_Manufacturing_CA and CAPF certificates Télécharger le fichier .pem et sauver comme un fichier .txt.

```
IOS: crypto pki trustpoint Trust_CUCM  
enrollment terminal  
crypto pki authenticate trustpoint
```

Coller le certificat en Base64. Idem pour les autres certificats.

CUCM – Configuration IOS

```
crypto key generate rsa general-keys label  
key_CUCM  
crypto pki trustpoint CUCM  
enrollment selfsigned  
rsa keypair CUCM 2048 2048  
authorization username subjectname commonname  
crypto pki enroll CUCM  
  
crypto pki export CUCM pem terminal
```

CUCM – Configuration IOS

Le logiciel pour le téléphone doit être installé sur le routeur :

```
webvpn install svc flash:/webvpn/anyconnect-win-2.3.2016-k9.pk
```

Pour utiliser le téléphone avec les deux certificats et l'authentification par mot de passe, créer un utilisateur avec l'adresse MAC du téléphone.

```
username CP-7975G-SEP001AE2BC16CB password  
k1kLGQIoxyC04ti9 encrypted
```

CUCM – Configuration ASA

Prérequis :

Installer ASA software (version 8.0.4 or later) et un ASDM compatible

Installer un package AnyConnect compatible

Activer la licence

CUCM – Configuration ASA

Step 2 Generate and register the necessary certificates for Unified Communications Manager and ASA.

Import the following certificates from the Unified Communications Manager.

- CallManager - Authenticating the Cisco UCM during TLS handshake (Only required for mixed-mode clusters).
- Cisco_Manufacturing_CA - Authenticating IP phones with a Manufacturer Installed Certificate (MIC).
- CAPF - Authenticating IP phones with an LSC.

To import these Unified Communications Manager certificates, do the following:

- a) From the Cisco Unified OS Administration, choose **Security > Certificate Management**.
- b) Locate the certificates Cisco_Manufacturing_CA and CAPF. Download the .pem file and save as a .txt file.
- c) Create trustpoint on the ASA.

Example:

```
ciscoasa(config)# crypto ca trustpoint trustpoint_name  
ciscoasa(ca-trustpoint)# enrollment terminal  
ciscoasa(config)# crypto ca authenticate trustpoint_name
```

When prompted for base 64 encoded CA Certificate, copy-paste the text in the downloaded .pem file along with the BEGIN and END lines. Repeat the procedure for the other certificates.

CUCM – Configuration ASA

Enregistrer le certificat prévu vers le CUCM

Sur ASA

```
crypto ca export <name> identity-certificate
```

Copier le texte dans un fichier .pem pour le télécharger sur le CUCM.

CUCM – Configuration ASA

```
username CP-7975G-SEP001AE2BC16CB password k1kLGQloxyCO4ti9  
encrypted
```

```
username CP-7975G-SEP001AE2BC16CB attributes vpn-group-policy  
GroupPhoneWebvpn service-type remote-access
```


Sur CUCM – Chargement d’un certificat

Depuis le OS Management du CUCM,
Choisir ‘**Security**’ / ‘**Certificate management**’

Cliquer sur ‘**Upload certificate**’ .
De ‘**Certificate Purpose**’
Choisissez **Phone-VPN-trust**

Choisir le fichier de certificat
et cliquer sur ‘**Upload**’.

Upload Certificate/Certificate chain

Upload Close

Status

i Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose* CallManager-trust

Description(friendly name)

Upload File Browse... SSL certificate.pem

Upload Close

Sur CUCM – Configuration de la passerelle VPN

Depuis l'[Administration du CUCM](#),

Choisir '**Advanced Feature**' / '**VPN**' / '**VPN gateway**'

Cliquer sur '**Add new**'

Puis sur '**Copy**'

Configurer la gateway
avec les bon paramètres :

Nom

Description

URL

Certificats

Cliquer sur '**Save**'

VPN Gateway Configuration Related Links: [Back T](#)

Save ✖ Delete Copy + Add New

Status

i Status: Ready

VPN Gateway Information

VPN Gateway Name*

VPN Gateway Description

VPN Gateway URL*

VPN Gateway Certificates

VPN Certificates in your Truststore

▼ ▲

VPN Certificates in this Location*

Save Delete Copy Add New

Sur CUCM – Configuration d'un Groupe VPN

Depuis l'[Administration du CUCM](#),
Choisir '**Advanced Feature**' /
'**VPN**' / '**VPN group**'

Cliquer sur '**Add new**'
Puis sur '**Copy**'

Configurer les paramètres :
Nom,
Description,
les Passerelles VPN disponibles

Cliquer sur '**Save**'

The screenshot shows the 'VPN Group Configuration' page in CUCM. At the top, there is a 'Save' button. Below it, the 'Status' section shows 'Status: Ready'. The 'VPN Group Information' section contains two text input fields: 'VPN Group Name*' with the value 'VPNGroup' and 'VPN Group Description' with the value 'VPNGroup'. The 'VPN Gateway Information' section features two list boxes. The first, 'All Available VPN Gateways', is currently empty. The second, 'Selected VPN Gateways in this VPN Group*', contains the entry 'VPNPhone'. Navigation arrows are visible between the two list boxes.

Sur CUCM – Configuration d'un Profil VPN

Depuis l'[Administration du CUCM](#),
Choisir '**Advanced Feature**' / '**VPN**'
/ '**VPN profil**'

Cliquer sur '**Add new**' Puis sur '**Copy**'

Configurer les paramètres :
Nom, Description, MTU, Fail to connect,
Enable Host ID check,
Client authentication Method,
Enable password persistence
Cliquer sur '**Save**'

VPN Profile Configuration

Save

Status

Status: Ready

VPN Profile Information

Name*

Description

Enable Auto Network Detect

Tunnel Parameters

MTU*

Fail to Connect*

Enable Host ID Check

Client Authentication

Client Authentication Method*

Enable Password Persistence

Save

Sur CUCM – Ajouter des détails du VPN au profil commun du téléphone

Depuis l'Administration du CUCM,
Choisir 'Device' / 'Device settings'
/ 'Common Phone Profil'

Cliquer sur 'Find'
Puis choisir le profil

Dans la section 'VPN information'
choisir les 'VPN Group'
et 'VPN Profile'.

Cliquer sur 'Save'
puis 'Apply Config' et 'OK'

Common Phone Profile Configuration

Save Delete Copy Reset Apply Config Add New

Status
Status: Ready

Common Phone Profile Information

Name*
Description
Local Phone Unlock Password
DND Option* Ringer Off
DND Incoming Call Alert* Beep Only
Feature Control Policy < None >
 Enable End User Access to Phone Background Image Setting

Secure Shell Information

Secure Shell User
Secure Shell Password

Phone Personalization Information

Phone Personalization* Default
Always Use Prime Line* Default
Always Use Prime Line for Voice Message* Default
Services Provisioning* Default

VPN Information

VPN Group
VPN Profile

Peut-on utiliser
AnyConnect avec le
CUCM en mode non
sécurisé ?

Polling Question - Sondage 5

- A. OUI
- B. NON



Avec Jabber

Références :

« Cisco AnyConnect Deployment Guide for Cisco Jabber October 2012 »

Et

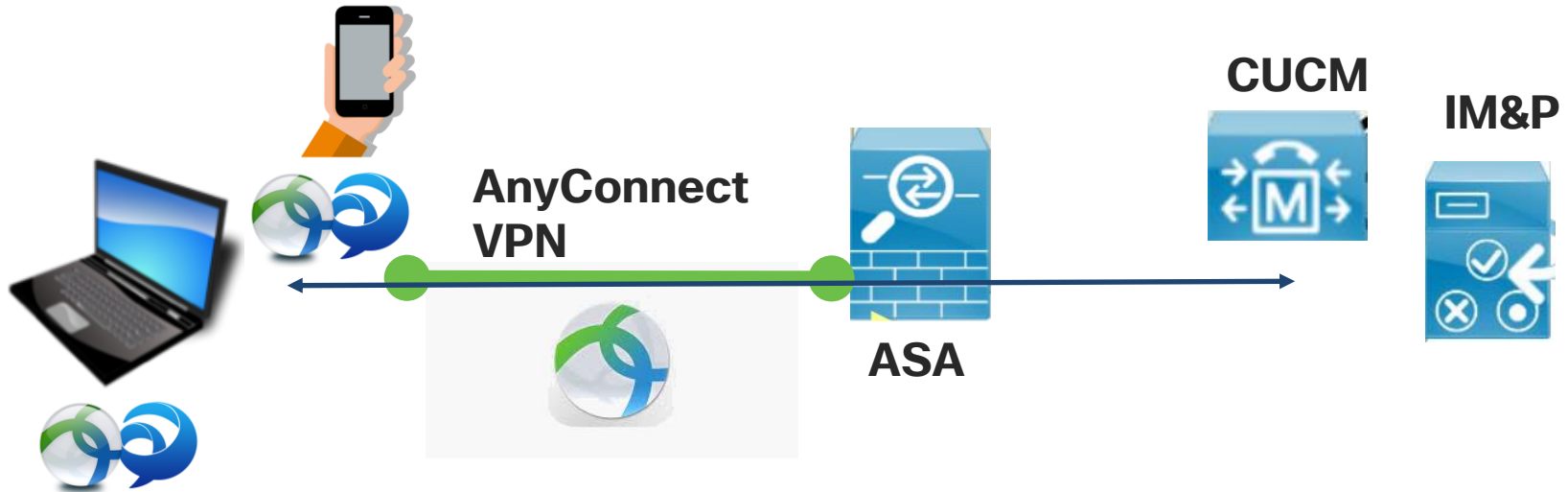
« On-Premises Deployment for Cisco Jabber 12.7 » Chapitre «**Remote Access** / Cisco Anyconnect Deployment Workflow »

Last Modified: 2020-08-18

(Beaucoup d'info. Spécifiques **iOS Apple** à lire)

Jabber

Le principe d'intégration ressemble beaucoup à ce que l'on trouve pour un ordinateur ou un smartphone pour les autres applications.



Application Profiles

Une fois le client AnyConnect installé, l'ASA doit lui envoyer son **profil**. -Ex :concentrateurs VPN, IPSec ou SSL-

Le profil peut être défini en mode CLI ou ASDM.

Il existe un mode de **connexion automatique** en arrière plan.

Trusted networks connexions

Permet la connexion automatique en fonction de la localisation.

Automatic VPN access on CUCM

Prérequis:

- on-demand access vers le VPN avec une authentification basée sur le certificat
- voir les documents « Software requirement » et « Cisco Anyconnect VPN Client Maintain and Operate Guide »

Procédure:

- 1) Identifier l'URL qui va déclencher le VPN on Demand

Automatic VPN access on CUCM

Procédure (Suite)

Si **Connect if Needed**

Configurer le CUCM pour l'accès à travers un nom de domaine (pas une @IP) . Pas de résolution hors le firewall.

Inclure le nom de domaine dans la liste « Connect if needed » dans le **Client AnyConnect**.

Automatic VPN access on CUCM

Procédure (suite):

Si **Always Connect**


- Le paramètre *On-Demand VPN URL* devrat être mis à un nom de domaine inexistant.
- Inclure le nom de domaine dans la liste « Connect if needed » dans le **Client AnyConnect**.
(l'URL doit être uniquement le nom de domaine)

Entrer l'URL dans Cisco AnyConnect et vérifier que l'interrogation DNS vers le domaine échoue.

Automatic VPN access on CUCM

Procédure (suite):

Dans la page CUCM / User / Product Specific Configuration Layout / *On-Demand VPN URL* entrez l'URL définie avant.



Product Specific Configuration Layout ?

Allow End User Configuration Editing	Enabled
Country Code	US
Cisco Usage and Error Tracking	Disabled
Enable Sip Digest Authentication	Disabled
Sip Digest Username	
Contacts	
On-Demand VPN URL	ccm-sjc-1.cisco.com
XML Options	

Sauvez la page.

Dissipez vos
doutes



Utilisez le panneau « Q&R » pour poser
vos questions

Cisco Community – Demandez-moi ...



Avez-vous encore des questions sur ce sujet ?

Foire aux Questions
jusqu'au vendredi 14 mai

avec Alain Faure
Événement public

Suivez le lien

<https://bit.ly/AMA-may21>

Ask Me Anything | Sécurité
Demandez-moi n'importe quoi !

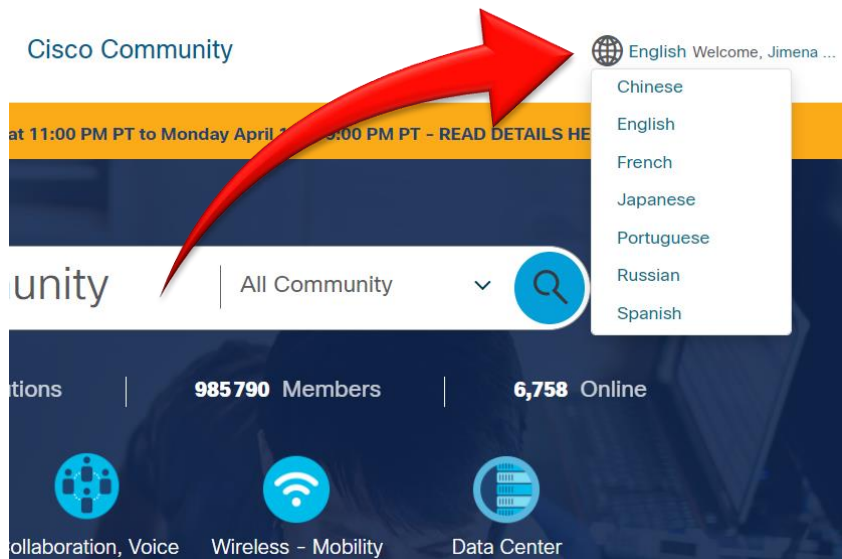
 **Posez une Question** >>

4 - 14 MAI
Alain Faure

Demandez-moi n'importe quoi
Le Télétravail : la Collaboration et l'Intégration RaVPN dans la Sécurité

La communauté est disponible dans d'autres langues

Si vous parlez l'anglais, l'espagnol, le portugais, le russe, le chinois ou le japonais, vous pouvez participer aussi dans les autres communautés Cisco !



Cisco Community

English Welcome, Jimena ...

- Chinese
- English
- French
- Japanese
- Portuguese
- Russian
- Spanish

Community | All Community

985790 Members | 6,758 Online

Collaboration, Voice | Wireless - Mobility | Data Center

- Anglais [Cisco Community](#)
- Espagnol [Comunidad de Cisco](#)
- Portugais [Comunidade da Cisco](#)
- Russe [Сообщество Cisco](#)
- Chinois [思科服务支持社区](#)
- Japonais [シスコ コミュニティ](#)

Nous vous invitons à nous suivre dans les réseaux sociaux et à partager nos prochains événements

Cisco Community

- Facebook/CiscoSupportCommunity
- Twitter @cisco_support
- YouTube ciscosupportchannel
- LinkedIn Cisco Community
<https://www.linkedin.com/showcase/3544800/>
- Instagram ciscosupportcommunity
<https://www.instagram.com/ciscosupportcommunity/>



Votre avis nous
intéresse !



Veillez remplir le sondage qui
apparaîtra sur votre écran à la fin
de cette présentation.



Merci pour votre participation !

