



Communauté Cisco

Firepower Threat Defense VPN

VPN avec MFA DUO et SGT ISE

Francesco Molino

Network and Security Consultant - CCIE R&S | SP | Security #35050

Xavier Crèvecoeur

Network and Security Consultant - CCIE Security #11010 | Firejumper Élite #135

20 juin 2019

Nouveautés et prochains événements



Communauté Cisco – Demandez à l'Expert

Principes fondamentaux de Commutation, configuration et meilleures pratiques

Disponible jusqu'au
21 juin 2019

avec Leonardo Peña
Événement tout public

Suivez le lien

<http://bit.ly/ATEem-juin19>



The banner features a background image of a man working at a desk with multiple computer monitors. A circular inset shows a portrait of Leonardo Peña. The text is overlaid on a blue and black background.

 **Événements**

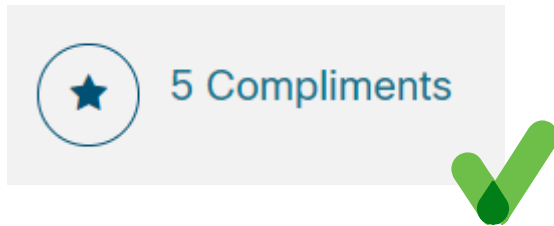
Demandez à un expert en Commutation !

Conduit par Leonardo Peña
Retrouvez-le dans la Communauté Cisco
Forum ouvert | Disponible jusqu'au 21 jun 2019.

Cliquez ici

Évaluez le contenu de la Communauté Cisco

Discussions, Documents, Blogs et Vidéos



Identifiez les experts



Repérez les solutions

Aidez-nous à identifier les contenus de qualité et à reconnaître l'effort des membres de la Communauté Cisco en français.

Reconnaissance aux Top Contributeurs



La reconnaissance aux **Top Contributeurs** est conçue pour reconnaître et remercier ceux qui ont collaboré avec nous en fournissant des contenus techniques de qualité ainsi que les participants plus actifs qui ont permis à notre communauté de devenir un des Top sites pour les passionnés de la technologie de Cisco.

Devenez un Top Contributeur

Spotlight Awards



The Community Spotlight Awards recognizes members whose significant contributions designate leadership and co- including Cisco Community, Cisco Learning Network (CLN), and Cisco Developers Network (CDN). Spotlight awards make our communities the premier online destination for Cisco enthusiasts. [FAQs](#)

2019 2018 2017 2016 2015 2014 2013 2012

January February **March** April May June July August September October November December

English Community Member's Choice



David Samuel Penalzo Seijas
2019 March

English Community Best Publication



Mohammad Khalil
2019 March



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



Les experts de la Communauté Cisco

Francesco Molino

Sr Network & Security Consultant

CCIE R&S, SP et Security
#35050



Présentateur

Les experts de la Communauté Cisco

Xavier Crèvecoeur

Sr Network & Security Consultant

CCIE Security #11010 &
Firejumper Elite #135



Q&R
Question Manager

Merci d'être avec
nous aujourd'hui !

Téléchargez la présentation sur

<http://bit.ly/WEBsId-jun19>



Nouveau chez Webex

The screenshot shows the Cisco Webex Events interface. At the top, there is a menu bar with options: File, Edit, Share, View, Communicate, Participant, Event, Help. Below the menu, the current event is titled "VS" and the host is "VIDHYA S (Cisco)". A sharing menu is open, showing "Sharing Screen /presso" with a dropdown arrow. A blue circle highlights this menu, and a blue arrow points from it to a blue callout box. The main content area displays a "VxLAN Overview" diagram. The diagram shows a central "IP Network (Underlay)" cloud connected to four "Edge Device" nodes. Each edge device is connected to a "Local LAN Segment", which in turn connects to "Physical Host" or "Virtual Hosts". A "Virtual Switch" is also shown connected to the edge devices. At the bottom of the interface, there is a navigation bar with icons for phone, video, share, record, profile, chat, and a red close button. A URL is visible at the bottom: <http://opendata.labs.lacnic.net/ipv6stats/graphs/ipv6evo.html>.

Assurez-vous de suivre la présentation dans l'onglet approprié.

Introduction

Cisco FTD, DUO Security et Cisco ISE

Francesco Molino, SBK Telecom,
CCIE R&S | SP | Security

Plus de 15 années d'expérience dans
les milieux des Télécommunications.
Fan inconditionnel des solutions
Cisco ☺ et Open-Sources.

Architecture de réseau
(LAN, WAN, Wi-Fi, Sécurité)

Déploiement et troubleshooting de
ces solutions.

Expérience et développement

Expérience au sein de projets
d'envergures pour des grandes
entreprises et Service Provider.

Développement d'outils d'automatisation
en utilisant les langages Python, Bash et
en s'appuyant également sur les APIs
fournies par les différents manufacturiers.

Objectif du webcast

L'objectif de ce webcast est de présenter la
solution Cisco Firepower Threat Defense et plus
particulièrement la fonctionnalité VPN AnyConnect
ainsi que l'interconnexion avec DUO Security (MFA)
et Cisco ISE pour une sécurité plus poussée.

Ordre du jour

- Architecture Firepower Threat Defense
- AnyConnect et ISE
- DUO Security
- Démonstration (laboratoire)

Polling question 1

Quelle est l'interface logique utilisée pour monter la connexion entre le FTD et FMC ?

- A. Interface br1
- B. Interface diagnostic
- C. N'importe quelle interface de data

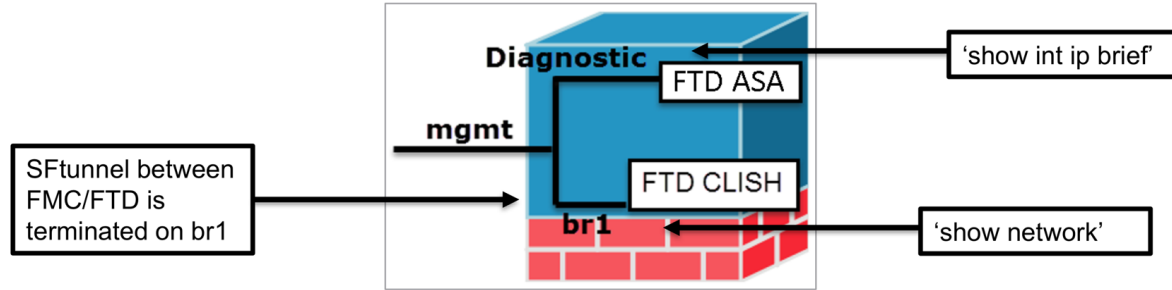


Firepower Threat Defense

Architecture

- Revue de l'architecture FTD

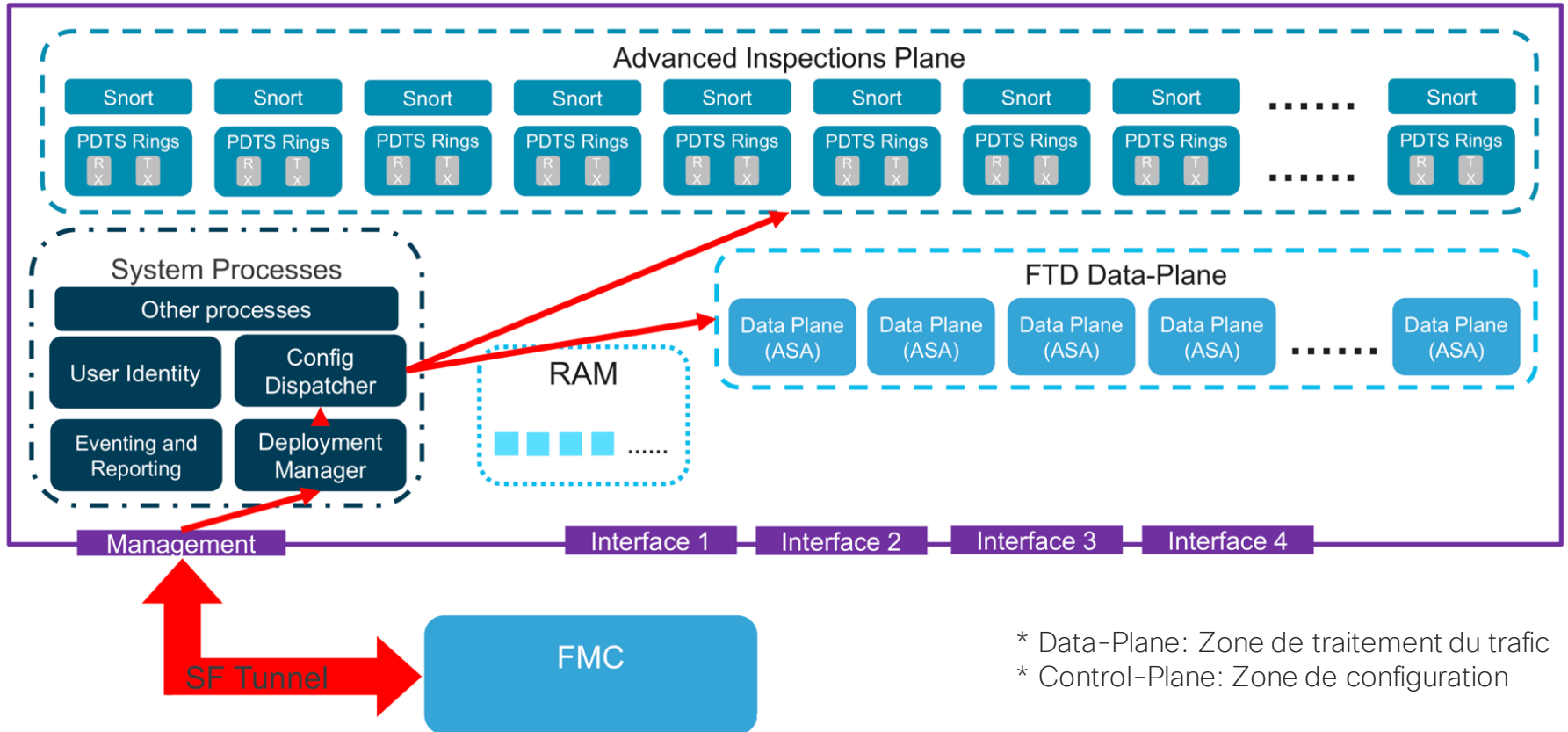
FTD – Interface de gestion (Management)



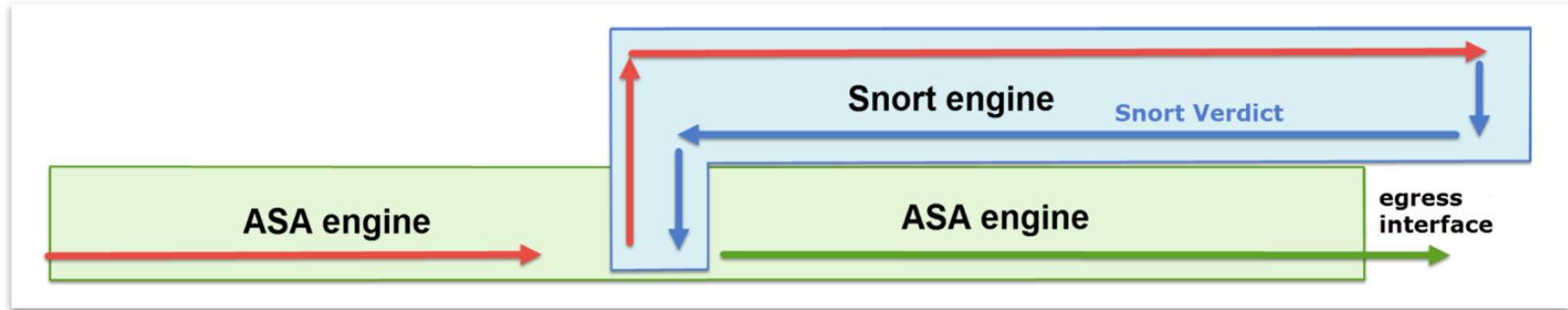
	br1	Diagnostic
Objectif	<ul style="list-style-type: none"> Utilisé pour monter le sftunnel (communication entre FMC et FTD) Permet de se connecter en SSH à l'équipement 	<ul style="list-style-type: none"> Accès SSH au moteur ASA Utilisé pour communiquer avec les serveurs Syslogs, AAA
Obligatoire	Oui (en outre car le sftunnel est terminé sur cette interface)	Non. Pas recommandé de l'utiliser et préférable d'utiliser une interface Data
Commande pour vérification	Show network (CLISH CLI)	Show interface IP brief (ASA CLI) (vu sous le nom Management 1/1)

* LINA = Système d'exploitation ASA

Firepower – Gestion de la configuration

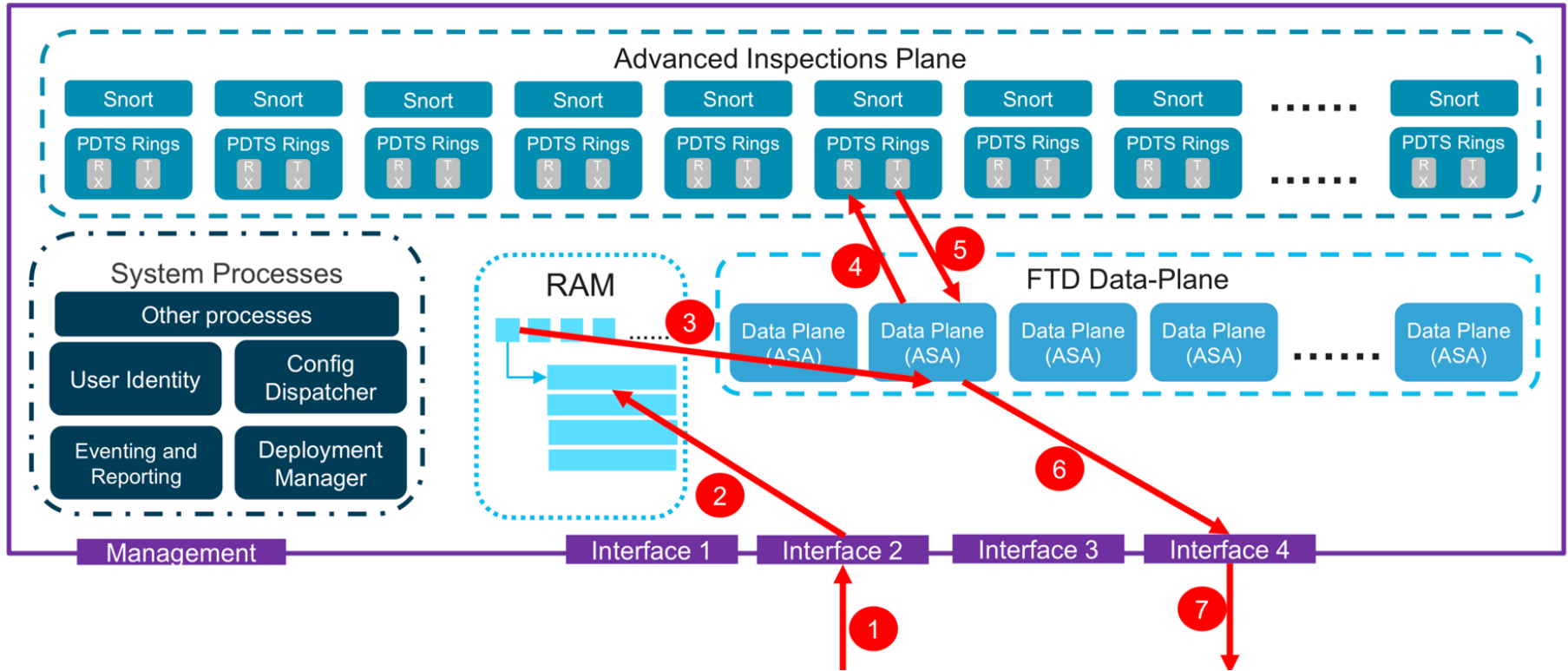


Firepower – Gestion du flux de trafic



1. Le paquet arrive sur l'interface d'entrée de l'ASA.
2. Si la règle identifiée pour traiter le trafic indique une inspection approfondie alors l'ASA transfère le trafic à l'engin SNORT.
3. En fonction du résultat de SNORT, le trafic est « drop » ou transféré vers l'interface de sortie.

Firepower – Gestion du flux de trafic



Firepower – Règle de pré-filtrage

Add Prefilter Rule ? X

ⓘ Prefilter rules perform early handling of traffic based on simple network characteristics. Fastpathed traffic bypasses access control and QoS.

Name: Enabled Insert: below rule 2

Action:

- Fastpath
- ✓ Analyze
- ✗ Block

Interface: Ports: Comment: Logging:

Available Interface Objects: Source Interface Objects (0): any Destination Interface Objects (0): any

3 actions pour le pré-filtrage :

- Block → Bloque le trafic
- Fastpath → Autorise le trafic et le traite entièrement dans le « Data Plane ».
 - Sur FP 4100 et 9300 le trafic peut être « offloadé » en utilisant le module « smart-nic » (static offload)
 - <https://community.cisco.com/t5/security-blogs/power-performance-with-dynamic-flow-offload-on-cisco-firepower/ba-p/3848826>
 - <https://www.youtube.com/watch?v=2qngILWhUuU>
- Analyze → Passe le trafic sur les règles principales pour l'évaluer

VPN

- AnyConnect

Firepower – AnyConnect

Dernière version en cours : 4.7.03052

Pas de parité en termes de fonctionnalités
AnyConnect entre ASA et FTD

AnyConnect supporte SSL and
IPSEC/IKEv2

- Avantage d'utiliser SSL: Fonctionne depuis n'importe quel endroit (même à travers des pare-feux et proxys)

AnyConnect ne supporte pas IKEv1

Peut être installé à travers :

- Du FTD (téléchargement)
- En mode installation automatique en utilisant des méthodes comme GPO...
- App-Store (Google et Apple)

Des modules supplémentaires :

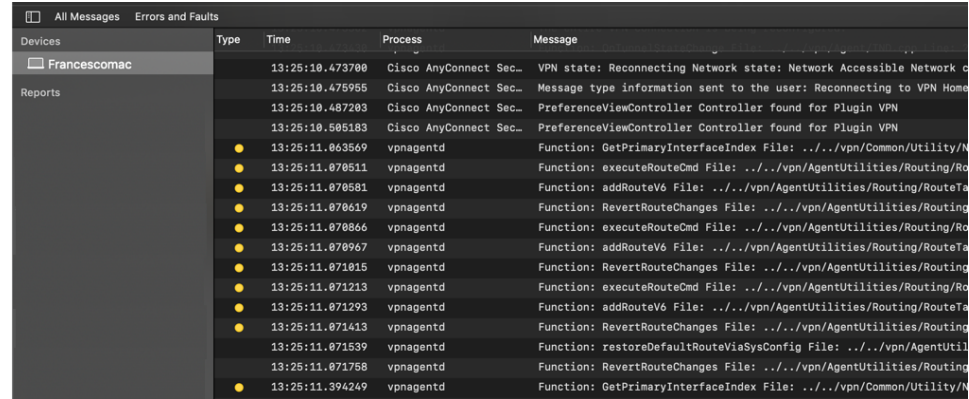
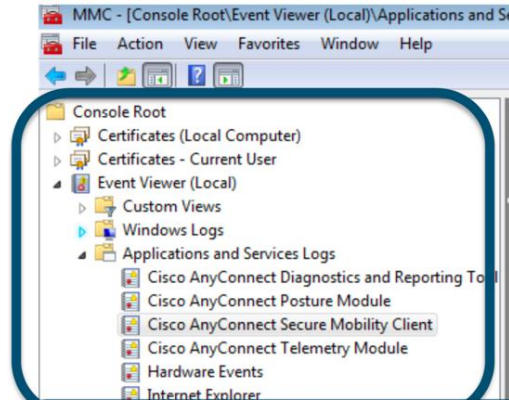
- DART (Outil de diagnostic)
- Posture
- AMP
- Umbrella ...

Firepower – AnyConnect Diagnostique

DART peut être installé uniquement sur MacOs et Windows

- Identique à un « show tech-support » mais côté client.
- Il récupère des données liées à l'OS et les logs AnyConnect puis les compresse dans un fichier zip pour les partager.

- Dans iOS et Android, AnyConnect intègre un « troubleshooting toolbox ».
- Ce « troubleshooting toolbox » est également intégré dans Windows et MacOs (journaux d'évènements pour Windows et Console pour MacOs).



Firepower – AnyConnect Redondance basée sur profile

Les profils AnyConnect peuvent être créés : (importés manuellement dans FTD/FMC)

- Depuis l'outil « VPN Profile Editor » (un poste Microsoft Windows est requis).
- Manuellement en créant un fichier xml (pour utilisateurs avancés si beaucoup d'options sont à configurer).

Dans le fichier xml ou depuis l'outil « VPN Profile Editor », il est possible d'ajouter un « backup server ».

The image displays three overlapping screenshots from the VPN Profile Editor interface:

- Top Left:** The 'Server List' table. The 'Backup Server List' column is highlighted with a red box, showing '-- Inherited --'. The table has columns: Hostname, Host Address, User Group, Backup Server List, SCEP, Mobile Se..., and Certificat... The first row contains 'TEST-VPN-PRIMAIRE' and 'test.vpn-primaire.ca'.
- Bottom Center:** The 'Server List Entry' dialog box. The 'Backup Servers' section at the bottom is highlighted with a red box, showing a 'Host Address' input field and an 'Add' button.
- Top Right:** The 'Backup Servers' configuration panel. The 'Backup Servers' menu item in the left sidebar is highlighted with a red box. The main panel shows a 'Host Address' input field and 'Add', 'Move Up', 'Move Down', and 'Delete' buttons.

Firepower – AnyConnect Redondance basée sur « profile »

Les profils AnyConnect peuvent être créés :

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
```

```
  <ServerList>
```

```
    <HostEntry>
```

```
      <HostName>TEST-VPN-PRIMAIRE</HostName>
```

```
      <HostAddress>test.vpn-primaire.ca</HostAddress>
```

```
      <BackupServerList>
```

```
        <HostAddress>test.vpn-secondaire.ca</HostAddress>
```

```
      </BackupServerList>
```

```
    </HostEntry>
```

```
  </ServerList>
```

```
</AnyConnectProfile>
```

Firepower – AnyConnect – Localisation du profile

The screenshot shows the Firepower configuration interface. On the left, a navigation pane lists various configuration options under 'Connection Profile', with 'Group Policies' selected. The main area displays 'Group Policies' with a table of existing policies. An 'Edit Group Policy' dialog box is open, showing the 'Name' field set to 'CERT-POLICY' and the 'Protocol' set to 'SSL'. The dialog has tabs for 'General', 'AnyConnect', and 'Advanced'. The 'AnyConnect' tab is active, showing 'Profiles' and 'Connection Settings' sections. The 'Profiles' section contains a description and a 'Client Profile' dropdown menu. Below the dropdown, there is a note about a standalone profile editor.

Name	Protocol
DfltGrpPolicy	SSL,IKEV2
CERT-POLICY	SSL

Edit Group Policy

Name:*

Description:

General **AnyConnect** **Advanced**

Profiles
AnyConnect profiles contains settings for the VPN client functionality and optional features. FTD deploys the profiles during AnyConnect client connection.

Connection Settings
Client Profile:

Standalone profile editor can be used to create a new or modify existing AnyConnect profile. You can download the profile editor from [Cisco Software Download Center](#).

Windows XP	%ALLUSERSPROFILE%\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
Windows Vista	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
Windows 7	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
Mac OS X	/opt/cisco/anyconnect/profile
Linux	/opt/cisco/anyconnect/profile

Firepower – AnyConnect: règles de pare-feu

Les utilisateurs VPN AnyConnect peuvent contourner les règles du pare-feu

- → Activer la fonctionnalité (sysopt permit-vpn)

Access Control for VPN Traffic

- Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)**
Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

Les utilisateurs VPN peuvent se voir attribuer un tag SGT (Security Group Tag) par Cisco ISE.

Si la fonctionnalité sysopt permit-vpn est activée, le filtrage d'accès basé sur SGT est inutile.

Firepower – AnyConnect AAA, LDAP et AD

FTD est compatible avec des solutions de MFA (« Multi-Factor Authentication ») :

- Cisco Duo Security
- OpenOTP
- ...

FTD supporte une authentification au travers des protocoles AAA et LDAP (pas de base de données d'utilisateurs locaux).

Authorization et Accounting ne sont pas supportés avec LDAP, AD.

Authentification par certificat supporté

- Livraison des certificats aux clients à travers de FTD non supportée

Firepower – AnyConnect limitations

Fonctionnalités non supportées:

- L'ensemble de fonctionnalités de Posture (hostscan, ISE endpoint posture...)
- « Customization and Localization »: Les fichiers nécessaires pour la personnalisation ne sont pas poussés par FTD
- « Custom attributes » comme par exemple « Deferred upgrade » (repousser la mise à jour du client AnyConnect par l'utilisateur), « Per-App VPN »
- Local CA on FTD
- SSO SAML2.0
- VPN Load Balancing
- TACACS, Kerberos (KCD Authentication and RSA SDI)

Polling question 2

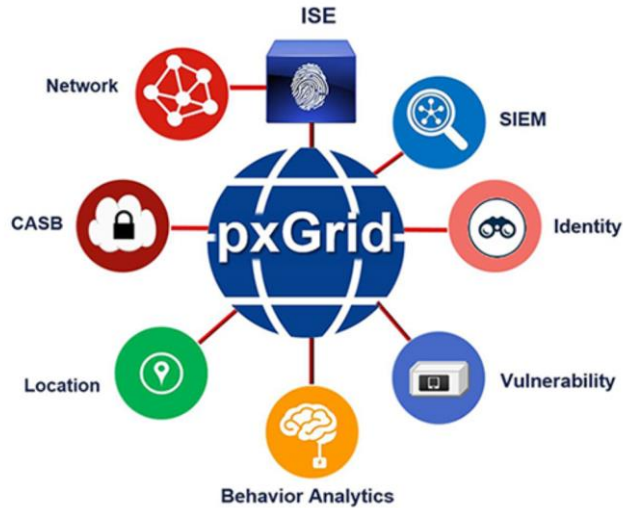
Comment s'appelle l'outil de diagnostic Cisco AnyConnect ?

- A. DRT
- B. DART
- c. Diagnostic Toolbox



FTD/FMC ISE PXGRID

Cisco Platform Exchange Grid (pxGrid)



FTD/FMC ISE PXGRID

FMC doit être interconnecté avec ISE.

Seule méthode d'interconnexion pour récupérer les informations liées aux tag SGT est PXGRID

The image shows two screenshots from the Cisco Identity Services Engine (ISE) management console. The left screenshot displays the 'Identity Sources' configuration page, and the right screenshot displays the 'pxGrid Services' monitoring page.

Identity Sources Configuration:

- Service Type: Identity Services Engine
- Primary Host Name/IP Address: 10.100.99.253
- Secondary Host Name/IP Address: (empty)
- pxGrid Server CA: ISE-PXGRID-CERT
- MNT Server CA: ISE-CERT
- FMC Server Certificate: FMC-CERT
- ISE Network Filter: (empty)

pxGrid Services Monitoring:

Client Name	Description	Capabilities	Status
ise-mnt-ise		Capabilities(2 Pub, 1 Sub)	Online (XMPP)
ise-pubsub-ise		Capabilities(0 Pub, 0 Sub)	Online (XMPP)
ise-bridge-ise		Capabilities(0 Pub, 4 Sub)	Online (XMPP)
ise-fanout-ise		Capabilities(0 Pub, 0 Sub)	Online (XMPP)
ise-admin-ise		Capabilities(5 Pub, 2 Sub)	Online (XMPP)
ia-fmc01.supportlan.com-2913c8...		Capabilities(0 Pub, 6 Sub)	Online (XMPP)

Capability Detail for ia-fmc01.supportlan.com-2913c8...:

Capability Name	Capability Version	Messaging Role
AdaptiveNetworkControl	1.0	Sub
Core	1.0	Sub
EndpointProfileMetaData	1.0	Sub
EndpointProtectionService	1.0	Sub
SessionDirectory	1.0	Sub
TrustSecMetaData	1.0	Sub

FTD/FMC ISE PXGRID - Certificats

Les certificats doivent être signés par la même autorité de confiance pour établir la communication.



FTD/FMC ISE PXGRID - Certificats

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

Edit Generate Self Signed Certificate Import Export Delete View

	Friendly Name	Used By	Portal group tag	Issued To	Issued By
<input type="checkbox"/>	OU=Certificate Services System Certificate,CN=ise.supportlan.com#Certificate Services Endpoint Sub CA - ise#00002	pxGrid		ise.supportlan.com	Certificate Services Endpoint Sub CA - ise
<input type="checkbox"/>	se.supportlan.com#Certificate Services Endpoint Sub CA - ise#00001	ISE Messaging Service		ise.supportlan.com	Certificate Services Endpoint Sub CA - ise
<input type="checkbox"/>	Default self-signed saml server certificate - CN=SAML_ise.supportlan.com	SAML		SAML_ise.supportlan.com	SAML_ise.supportlan.com
<input type="checkbox"/>	Default self-signed server certificate	Portal_RADIUS_DTLS	Default Portal Certificate Group	ise.supportlan.com	ise.supportlan.com
<input type="checkbox"/>	ISE Supportlan Signed Cert	Admin, EAP Authentication, Portal	PORTAL_LOCAL_SIGNED	ise.supportlan.com	supportlan-WINSRV-CA

* Certificat PXGRID: Le modèle de certificat doit contenir les EKU (Enhanced Key Usage) Client et Serveur authentication. Il peut s'appuyer sur le modèle de certificat « Web Server » enrichi du EKU Client authentication.

FTD/FMC ISE PXGRID - Certificats

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

All Clients Web Clients Capabilities Live Log Settings Certificates Permissions

Generate pxGrid Certificates

I want to *

- Generate a single certificate (without a certificate signing request)
- Generate a single certificate (with certificate signing request)
- Generate bulk certificates
- Download Root Certificate Chain

Common Name (CN) *

Certificate Template pxGrid_Certificate_Template ⓘ

Subject Alternative Name (SAN) [] [] - +

Certificate Download Format * [] ⓘ

Identity Services Engine Administration Work Centers License Warning

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

Issued Certificates

View Revoke

1 - 1 of 1 Show 25 per page Page 1 Show Quick Filter

Friendly Name	Device Unique Id	Serial Number	Valid From (yyyy-mm-dd)	Valid To (yyyy-mm-dd)	Issued By	Issued To	Status	Cert. Template
fmc.supportlan.com	10.100.99.249	340bac6ac940464...	2019-06-04	2021-06-04	CN=Certificate Service...	CN=fmc.supportlan.com	Active	pxGrid_Certificate_...

Firepower – Gestion des SGT

La gestion des SGT s'effectue depuis Cisco ISE.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'TrustSec' menu is expanded, showing options like 'BYOD', 'Profiler', 'Posture', 'Device Administration', and 'PassiveID'. The 'Components' menu is also expanded, showing 'TrustSec Policy', 'Policy Sets', 'SXP', 'Troubleshoot', 'Reports', and 'Settings'. The left sidebar contains 'Security Groups', 'IP SGT Static Mapping', 'Security Group ACLs', 'Network Devices', and 'Trustsec AAA Servers'. The main content area is titled 'Security Groups' and includes a link for 'Policy Export'. Below the title, there are action buttons: 'Edit', 'Add', 'Import', 'Export', 'Trash', 'Push', and 'Verify Deploy'. A table lists the Security Groups, with a red box highlighting the table content.

Icon	Name	SGT (Dec / Hex)	Description
	Auditors	9/0009	Auditor Security Group
	BYOD	15/000F	BYOD Security Group
	Contractors	5/0005	Contractor Security Group
	Developers	8/0008	Developer Security Group
	Development_Servers	12/000C	Development Servers Security Group
	Employees	4/0004	Employee Security Group
	Guests	6/0006	Guest Security Group
	Network_Services	3/0003	Network Services Security Group

Firepower – AnyConnect SGT

- Il est possible de pousser un tag SGT depuis Cisco ISE pour les utilisateurs VPN.

The screenshot shows the configuration page for a rule named 'MFA-ALLOW'. The rule is active (green checkmark) and its conditions are 'DEVICE:Device Type EQUALS All Device Types#FTD'. The action is 'PermitAccess'. On the right side, the 'Security Groups' dropdown menu is highlighted with a red box, showing 'Employees' as the selected group. The 'Hits' column shows a count of 5.

- Les tags SGT ne sont pas visibles sur les sessions en cours. Ils sont visibles en fin de session ou sur des actions de blocage.

The top screenshot shows a session log entry for a blocked session on 2019-06-06 at 21:22:18. The action is 'Block'. The initiator IP is 10.100.255.10 and the responder IP is 10.100.99.2. The security intelligence category is 'No Authentication Required'. The 'Security Group Tag' field is highlighted with a red box and contains the value 'Employees'. The access control rule is 'DENY-TEST-SGT'.

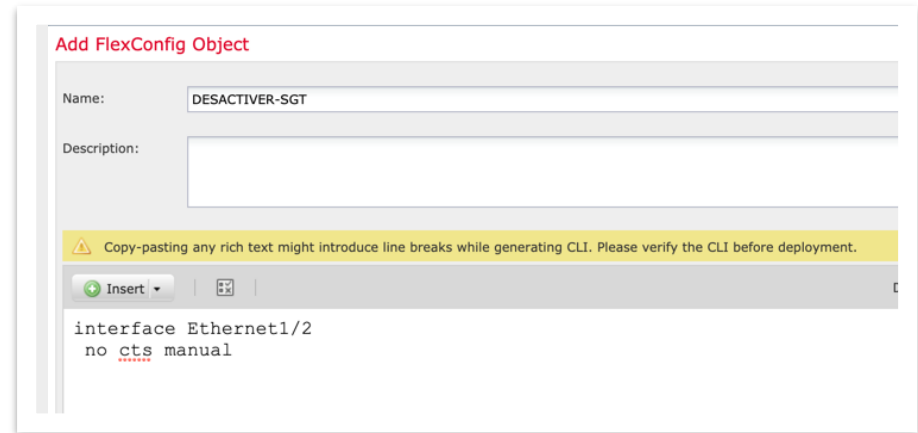
The bottom screenshot shows a session log entry for an allowed session on 2019-06-15 at 17:27:21. The action is 'Allow'. The initiator IP is 10.100.255.10 and the responder IP is 10.100.99.1. The security intelligence category is 'No Authentication Required'. The 'Security Group Tag' field is highlighted with a red box and contains the value 'Employees'. The access control policy is 'HOME-POLICY' and the access control rule is 'ANYCONNECT-ALLOW-LAN'.

Firepower – Attention SGT

FTD active par défaut le « native SGT tagging » sur les interfaces.

Cela peut avoir une incidence sur votre architecture sauf si les équipements derrière les interfaces ne supportent pas SGT.

- interface Ethernet1/2
- nameif INTERCO
- cts manual
- propagate sgt preserve-untag
- policy static sgt disabled trusted
- security-level 0
- ip address 10.100.254.5 255.255.255.252



Add FlexConfig Object

Name:

Description:

⚠ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

```
interface Ethernet1/2
no cts manual
```

Ces tags peuvent être désactivés à l'aide de Flexconfig.

Firepower – Dépannage

Plusieurs méthodes de « troubleshooting » :

- Depuis FMC, Device/VPN/Troubleshooting
- CLI (show vpn-sessiondb detail anyconnect)
- CLI (packet-tracer)
- CLI (capture packets)

Firepower – Dépannage: Depuis FMC

VPN Troubleshooting

Table View of VPN Troubleshooting

2019-06-06 09:02:00 - 2019-06-06 21:32:36

Expanding

Search Constraints (Edit Search)

Disabled Columns

<input type="checkbox"/>	Time	Severity	Message	Message Class	Username	Device
<input type="checkbox"/>	2019-06-06 21:32:27	Info	Group <CERT-POLICY> User <francesco> IP <204.48.93.58> UDP SVC connection established without compression	SSL VPN Client	francesco	FTD-HOME
<input type="checkbox"/>	2019-06-06 21:32:27	Notice	Group <CERT-POLICY> User <francesco> IP <204.48.93.58> First UDP SVC connection established for SVC session.	SSL VPN Client	francesco	FTD-HOME
<input type="checkbox"/>	2019-06-06 21:32:27	Info	Device completed SSL handshake with client INTERNET:204.48.93.58/61520 to 192.168.2.254/443 for DTLSv0.9 session	SSL Stack		FTD-HOME
<input type="checkbox"/>	2019-06-06 21:32:27	Info	SSL client INTERNET:204.48.93.58/61520 to 192.168.2.254/443 request to resume previous session	SSL Stack		FTD-HOME
<input type="checkbox"/>	2019-06-06 21:32:27	Info	Starting SSL handshake with client INTERNET:204.48.93.58/61520 to 192.168.2.254/443 for DTLS session	SSL Stack		FTD-HOME
<input type="checkbox"/>	2019-06-06 21:32:27	Info	Starting SSL handshake with client INTERNET:204.48.93.58/61520 to 192.168.2.254/443 for DTLS session	SSL Stack		FTD-HOME
<input type="checkbox"/>	2019-06-06 21:32:27	Info	SSL session with client INTERNET:204.48.93.58/47022 to 192.168.2.254/443 terminated	SSL Stack		FTD-HOME
<input type="checkbox"/>	2019-06-06 21:32:26	Info	AAA user accounting successful : server = 10.100.99.253 : user = francesco	User Authentication	francesco	FTD-HOME
<input type="checkbox"/>	2019-06-06 21:32:26	Warning	Group <CERT-POLICY> User <francesco> IP <204.48.93.58> IPv4 Address <10.100.255.10> IPv6 address <::> assigned to session	SSL VPN Client		FTD-HOME
<input type="checkbox"/>	2019-06-06 21:32:26	Info	Group <CERT-POLICY> User <francesco> IP <204.48.93.58> Client Type: Cisco AnyConnect VPN Agent for Apple iPhone 4.7.03051	SSL VPN Client		FTD-HOME
<input type="checkbox"/>	2019-06-06 21:32:26	Info	Group <CERT-POLICY> User <francesco> IP <204.48.93.58> TCP SVC connection established without compression	SSL VPN Client	francesco	FTD-HOME
<input type="checkbox"/>	2019-06-06 21:32:26	Notice	Group <CERT-POLICY> User <francesco> IP <204.48.93.58> First TCP SVC connection established for SVC session.	SSL VPN Client	francesco	FTD-HOME
<input type="checkbox"/>	2019-06-06 21:32:26	Warning	TunnelGroup <CERTIFICATE-PROFILE> GroupPolicy <CERT-POLICY> User <francesco> IP <204.48.93.58> No IPv6 address available for SVC connection	SSL VPN Client	francesco	FTD-HOME
<input type="checkbox"/>	2019-06-06 21:32:26	Notice	IPAA: Session=0x0557e000, IPv6 address: callback failed during IPv6 request	IP Address Assignment		FTD-HOME
<input type="checkbox"/>	2019-06-06 21:32:26	Notice	IPAA: Session=0x0557e000, IPv6 address: no IPv6 address available from local pools	IP Address Assignment		FTD-HOME
<input type="checkbox"/>	2019-06-06 21:32:26	Info	IPAA: Session=0x0557e000, Local pool request succeeded for tunnel-group 'CERTIFICATE-PROFILE'	IP Address Assignment		FTD-HOME
<input type="checkbox"/>	2019-06-06 21:32:26	Info	IPAA: Session=0x0557e000, Client assigned 10.100.255.10 from local pool HOME-VPN-POOL	IP Address Assignment		FTD-HOME
<input type="checkbox"/>	2019-06-06 21:32:26	Notice	IPAA: Session=0x0557e000, DHCP configured, no viable servers found for tunnel-group 'CERTIFICATE-PROFILE'	IP Address Assignment		FTD-HOME
<input type="checkbox"/>	2019-06-06 21:32:26	Info	Device completed SSL handshake with client INTERNET:204.48.93.58/59889 to 192.168.2.254/443 for TLSv1.2 session	SSL Stack		FTD-HOME
<input type="checkbox"/>	2019-06-06 21:32:26	Info	Device selects trust-point HOME-VPN-CERT-SELF-SIGNED for client INTERNET:204.48.93.58/59889 to 192.168.2.254/443	SSL Stack		FTD-HOME
<input type="checkbox"/>	2019-06-06 21:32:26	Info	Starting SSL handshake with client INTERNET:204.48.93.58/59889 to 192.168.2.254/443 for TLS session	SSL Stack		FTD-HOME
<input type="checkbox"/>	2019-06-06 21:32:26	Info	Device selects trust-point HOME-VPN-CERT-SELF-SIGNED for client INTERNET:204.48.93.58/47022 to 192.168.2.254/443	SSL Stack		FTD-HOME
<input type="checkbox"/>	2019-06-06 21:32:26	Info	Group <CERT-POLICY> User <francesco> IP <204.48.93.58> AnyConnect parent session started.	User Authentication		FTD-HOME
<input type="checkbox"/>	2019-06-06 21:32:26	Info	DAP: User francesco, Addr 204.48.93.58, Connection AnyConnect: The following DAP records were selected for this connection: DfltAccessPolicy	dap		FTD-HOME
<input type="checkbox"/>	2019-06-06 21:32:26	Info	AAA transaction status accept : user = francesco	User Authentication	francesco	FTD-HOME

Firepower – Dépannage :

show vpn-sessiondb

```
ftd# sh vpn-sessiondb detail anyconnect filter name francesco
```

Session Type: AnyConnect Detailed

Username : **francesco** Index : 21886
Assigned IP : 10.100.255.10 Public IP : 204.48.93.58
Protocol : AnyConnect-Parent SSL-Tunnel
License : AnyConnect Premium, AnyConnect for Mobile
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384
Bytes Tx : 29774 Bytes Rx : 9471
Pkts Tx : 125 Pkts Rx : 129
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : CERT-POLICY Tunnel Group : CERTIFICATE-PROFILE
Login Time : 01:32:21 UTC Fri Jun 7 2019
Duration : 0h:40m:37s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : c0a802fe0557e0005cf9bea5
Security Grp : 4 Tunnel Zone : 0

AnyConnect-Parent Tunnels: 1

SSL-Tunnel Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 21886.1
Public IP : xxx.xxx.xxx.xxx
Encryption : none Hashing : none
TCP Src Port : 47022 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 0 Minutes
Conn Time Out: 600 Minutes Conn TO Left : 559 Minutes
Client OS : apple-ios
Client OS Ver: 12.4
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Apple iPhone 4.7.03051
Bytes Tx : 5472 Bytes Rx : 0
Pkts Tx : 6 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 21886.6
Assigned IP : 10.100.255.10 Public IP : xxx.xxx.xxx.xxx
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 52614
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Conn Time Out: 600 Minutes Conn TO Left : 559 Minutes
Client OS : Apple iOS
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Apple iPhone 4.7.03051
Bytes Tx : 13530 Bytes Rx : 6288
Pkts Tx : 71 Pkts Rx : 81
Pkts Tx Drop : 0 Pkts Rx Drop : 0

Firepower – Dépannage: packet-tracer

```
ftd# packet-tracer input INTERNET icmp 10.100.255.10 8 0 10.100.99.2
```

```
Mapping security-group 4 to IP address 10.100.255.10
```

Phase: 1

Type: UN-NAT

Subtype: static

Result: ALLOW

Config:

```
nat (INTERCO,INTERNET) source static My-Networks My-Networks destination static ANYCONNECT-VPN-SUBNET ANYCONNECT-VPN-SUBNET
```

```
description ANYCONNECT-VPN
```

Additional Information:

```
NAT divert to egress interface INTERCO
```

```
Untranslate 10.100.99.2/0 to 10.100.99.2/0
```

Phase: 2

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

```
access-group CSM_FW_ACL_ global
```

```
access-list CSM_FW_ACL_ advanced permit ip ifc INTERNET any ifc INTERCO object DHCP-SRV rule-id 268437510
```

```
access-list CSM_FW_ACL_ remark rule-id 268437510: ACCESS POLICY: HOME-POLICY - Default
```

```
access-list CSM_FW_ACL_ remark rule-id 268437510: L7 RULE: DENY-TEST-SGT
```

Additional Information:

```
This packet will be sent to snort for additional processing where a verdict will be reached
```

DUO Security

- MFA

FMC - DUO - Qu'est ce que Duo Security ?

Multi-Factor Authentication (MFA)

Broadest range of authentication methods for your users



Push



Soft Token



SMS



Phone Call



U2F



Wearables



Biometrics



HW Tokens

One-tap login



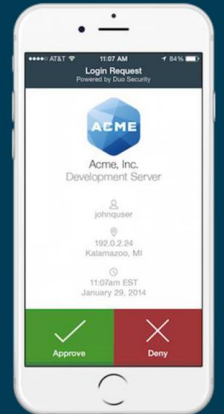
Duo Push

Value

- Easy to use and Easy to rollout
- Security asymmetric cryptography
- Out-of-band

Key Considerations

- iOS, Android
- Timeout 60s
- Private key is stored securely on the mobile device



FMC - DUO - ISE

FTD VPN avec MFA et Duo peut être déployé de plusieurs façons :

- Configuration de 2 serveurs d'authentications pour obtenir le champ supplémentaire sur AnyConnect (SGT disponible)
- Utiliser Duo seulement comme serveur Radius (SGT non disponible)
- Utiliser ISE comme Proxy Radius qui transfère la requête au serveur Duo (SGT disponible)

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes Home, Context Visibility, Operations, Policy, and Administration. Under Administration, the path is System > Identity Management > Network Resources > Network Devices. The main content area displays a table of Network Devices with columns for Name, IP/Mask, Profile Name, and Location. Two devices are listed: DUO and FTD, both with IP addresses in the 10.100.x.x range and Profile Name 'Cisco'. The DUO and FTD rows are highlighted with a red box.

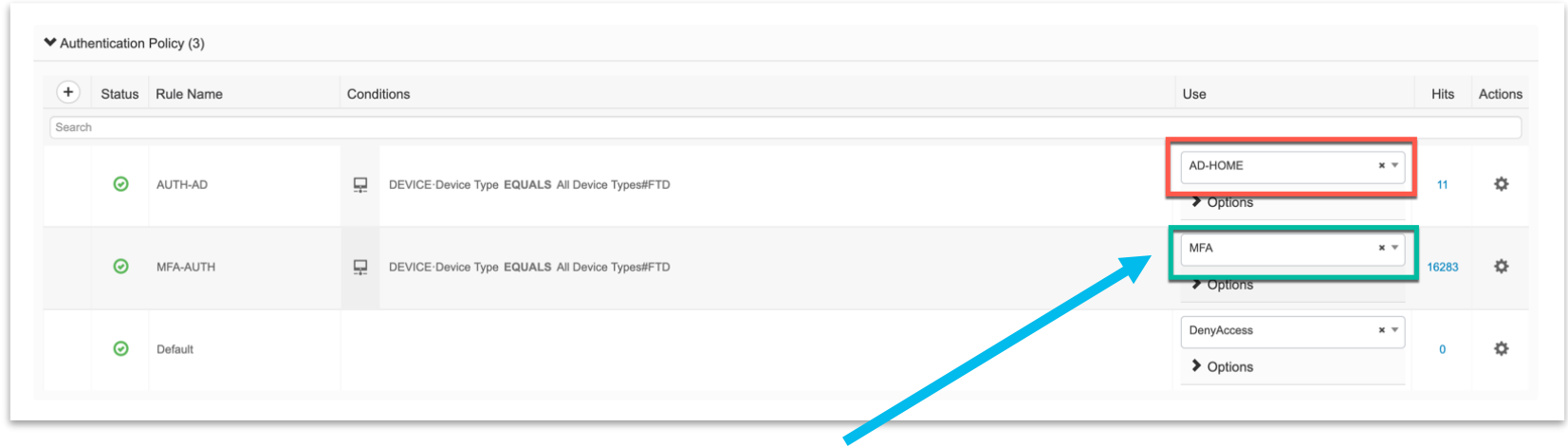
Name	IP/Mask	Profile Name	Location
<input type="checkbox"/> DUO	10.100.99.2/32	Cisco	Internal
<input type="checkbox"/> FTD	10.100.254.5/32	Cisco	External

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes Home, Context Visibility, Operations, Policy, and Administration. Under Administration, the path is System > Identity Management > External Identity Sources. The main content area displays a tree view of External Identity Sources. The 'RADIUS Token' folder is expanded, and the 'DUO' entry is highlighted with a red box. To the right, the 'RADIUS Token Identity Sources' configuration page is visible, showing the 'Name' field set to 'DUO'.

External Identity Sources

- Certificate Authentication Profile
- Active Directory
 - AD-HOME
- LDAP
- ODBC
- RADIUS Token**
 - DUO**
 - RSA SecurID
 - SAML Id Providers
 - Social Login

FMC - DUO - ISE



Authentication Policy (3)						
+	Status	Rule Name	Conditions	Use	Hits	Actions
	✔	AUTH-AD	DEVICE:Device Type EQUALS All Device Types#FTD	AD-HOME	11	⚙️
	✔	MFA-AUTH	DEVICE:Device Type EQUALS All Device Types#FTD	MFA	16283	⚙️
	✔	Default		DenyAccess	0	⚙️

- Si ISE est utilisé comme proxy radius, nous déclarons une règle d'authentification qui devra utiliser le serveur Duo (déclarer comme serveur externe).

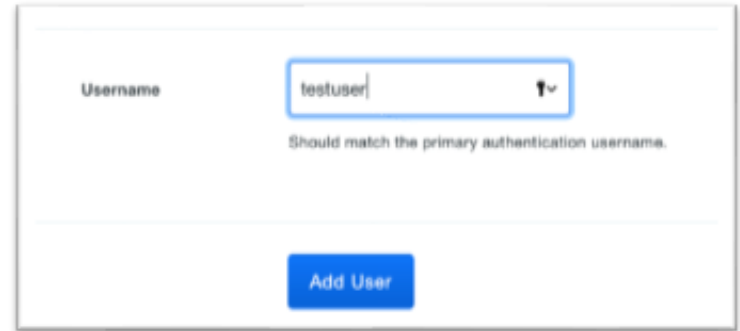
DUO Security – Configuration Portail

Les utilisateurs peuvent être synchronisés avec Azure Directory ou Active Directory

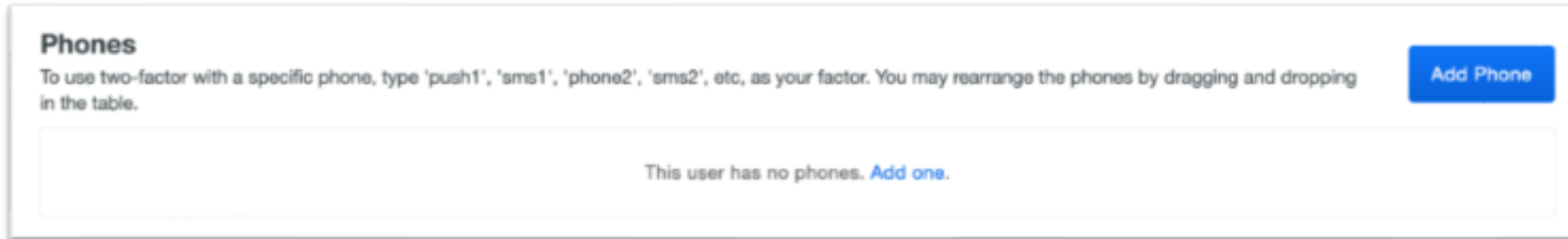
- <https://duo.com/docs/directorysync>

Les utilisateurs peuvent être créés localement sur le portail Duo.com

- Création de comptes 1 par 1
- Import en mode « bulk » (csv import)



A screenshot of a web form for adding a user. The form has a label "Username" on the left. To its right is a text input field containing "testuser" and a dropdown arrow icon. Below the input field is the text "Should match the primary authentication username." At the bottom of the form is a blue button labeled "Add User".



A screenshot of a web form section titled "Phones". Below the title is the text: "To use two-factor with a specific phone, type 'push1', 'sms1', 'phone2', 'sms2', etc, as your factor. You may rearrange the phones by dragging and dropping in the table." To the right of this text is a blue button labeled "Add Phone". Below the text is a large empty rectangular box. At the bottom of this box is the text: "This user has no phones. [Add one.](#)"

DUO Security – Configuration Portail (inscription)

Type Phone Tablet

Phone number [Show extension field](#)

[Add Phone](#)

Activate Duo Mobile

This form allows you to generate a new activation code for this phone's Duo Mobile application. The D passcodes on their mobile device or authenticate via Duo Push.

Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this device i

Phone 438-438-2932

Expiration after generation

[Generate Duo Mobile Activation Code](#)



testuser

[Attach a user](#)

Authentication devices
can share multiple
users

Device Info



Not using Duo Mobile
[Activate Duo Mobile](#)



Model
Unknown

DUO Security - MFA

FTD supporte MFA « Multi Factor Authentication » dont Duo, RSA, OpenOTP

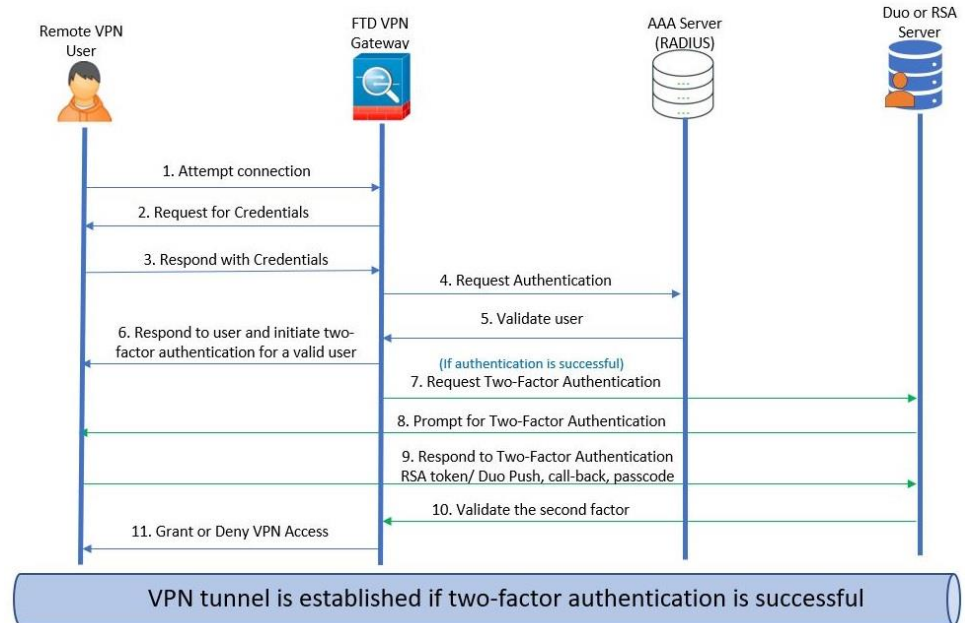
FTD ne supporte pas l'accès à Duo en mode LDAPS.

Seul mode supporté est Duo Radius Proxy avec les différents types de méthodes :

- SMS
- Push
- Duo-Passcode

DUO Radius Proxy (Windows et/ou Linux)

- Intégration avec serveur LDAP et Radius



DUO Security – Configuration

Fichier de configuration : authproxy.cfg

MFA seulement

```
[radius_server_duo_only]
ikey=ikey
skey=skey
api_host=api.duosecurity.com
radius_ip_1=xx.xx.xx.xx
radius_secret_1=radius-secret1
radius_ip_2=xx.xx.xx.xx
radius_secret_2=radius-secret2
client=duo_only_client
pass_through_all=true
port=1812
failmode=safe
```

Radius Server et LDAP

```
[ad_client]
host=xx.xx.xx.xx
service_account_username=duosecurity
service_account_password=password
search_dn=DC=testad,DC=com
security_group_dn=CN=VPN,OU=users,DC=testad,DC=com

[radius_server_auto]
ikey=ikey
skey=skey
api_host=api.duosecurity.com
radius_ip_1=xx.xx.xx.xx
radius_secret_1=radius-secret1
radius_ip_2=xx.xx.xx.xx
radius_secret_2=radius-secret2
client=ad_client
pass_through_all=true
port=1812
failmode=safe
```

DUO Security - Dépannage

Fichier de log : authproxy.log

```
2019-06-07T20:04:54-0400 [-] DuoForwardServer starting on 1812
2019-06-07T20:04:54-0400 [-] Starting protocol <duoauthproxy.lib.forward_serv.DuoForwardServer object at 0x034BF7D0>
2019-06-07T20:04:54-0400 [-] FIPS mode is not enabled
2019-06-07T20:04:54-0400 [-] RADIUS Duo-Only Server Module Configuration:
2019-06-07T20:04:54-0400 [-] {'api_host': 'api-████████.duosecurity.com',
    'client': 'duo_only_client',
    'failmode': 'safe',
    'ikey': '████████████████████',
    'pass_through_all': 'true',
    'port': '1812',
    'radius_ip_1': '10.100.99.253',
    'radius_ip_2': '10.100.254.5',
    'radius_secret_1': '*****',
    'radius_secret_2': '*****',
    'skey': '*****[40]'}
2019-06-07T20:04:54-0400 [-] Duo Security Authentication Proxy 3.0.0 - Init Complete
```

Polling question 3

Quelle est la méthode d'authentification non supportée par AnyConnect sur FTD ?

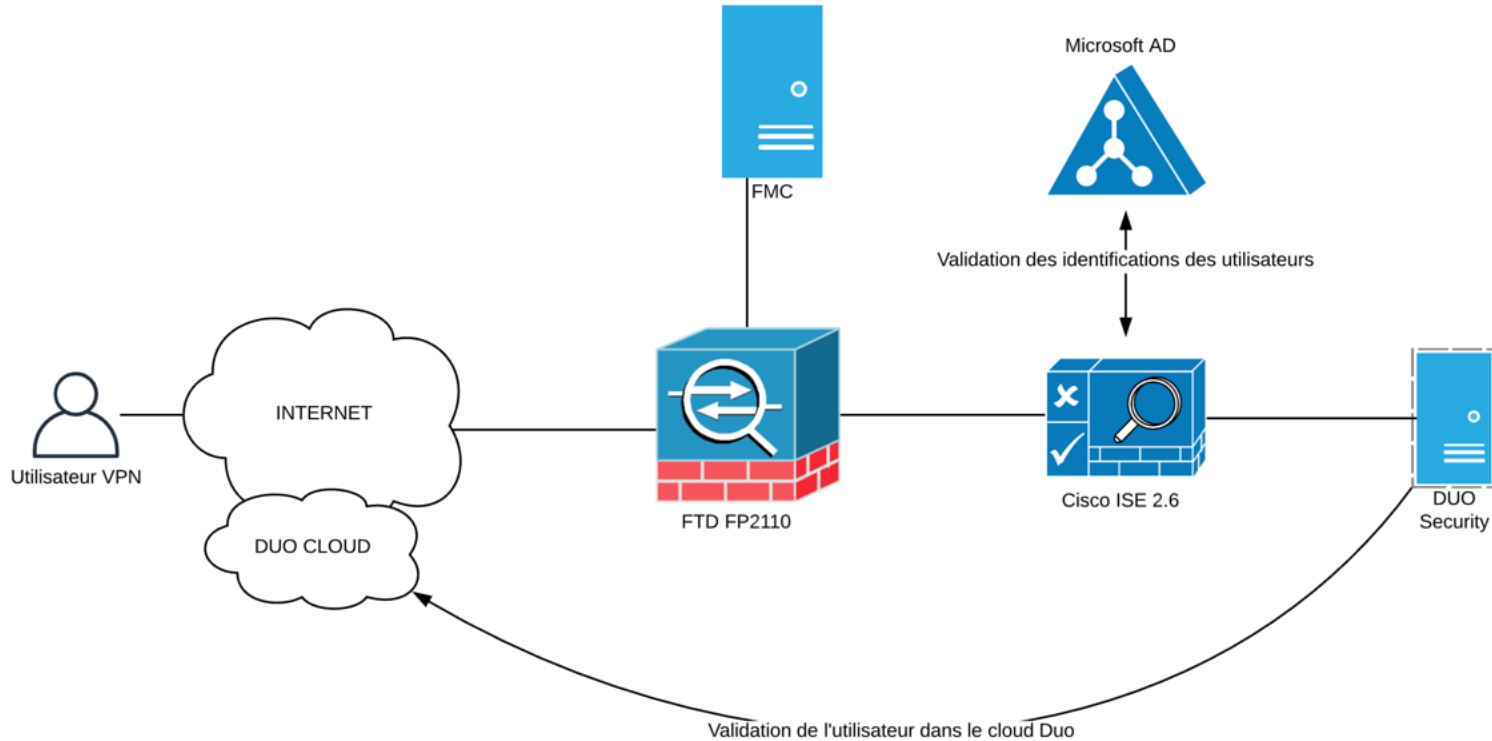
- A. LDAP
- B. Radius
- C. SSO SAML2.0



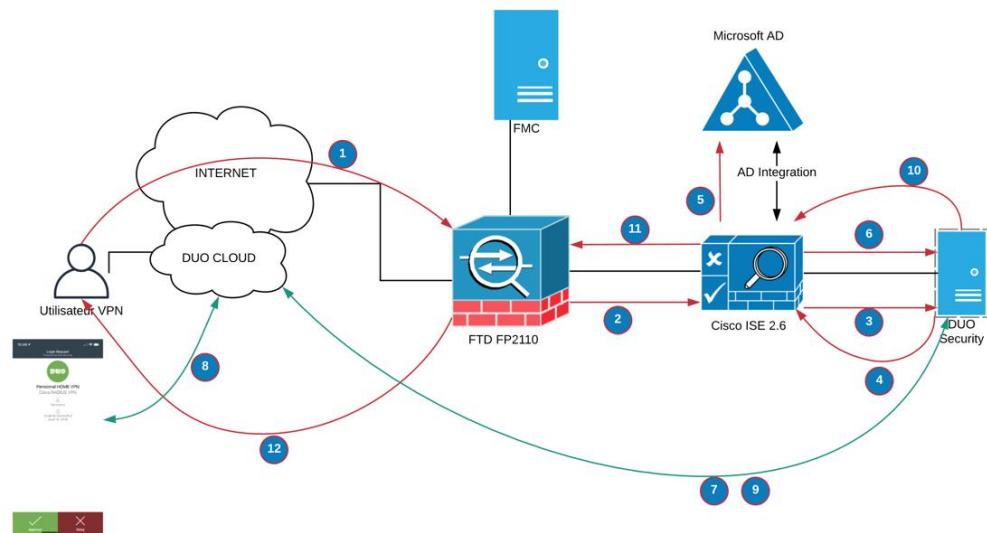
Démonstration



Démo - architecture à très haut niveau

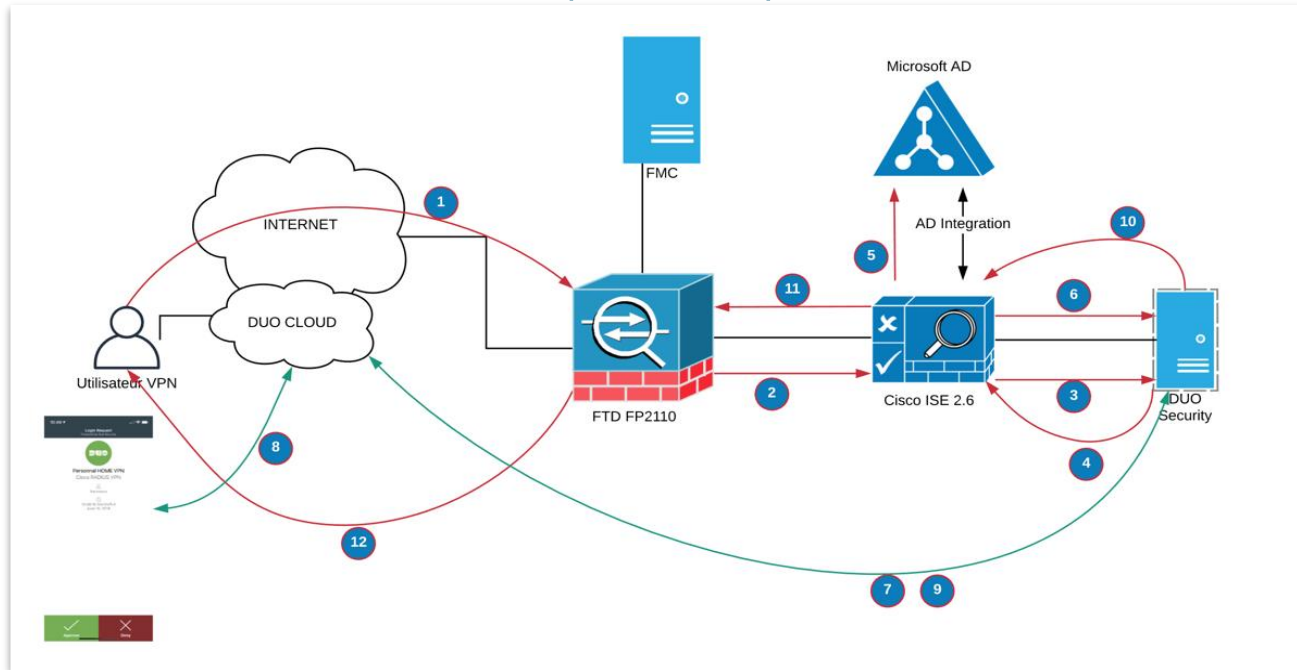


Démo – Flux de trafic (Légende)



Étapes	Description
1	Utilisateur demande une connexion VPN
2	FTD reçoit la demande et transfère à ISE
3	ISE renvoie la demande au Proxy Duo (Radius)
4	Duo authentifie l'utilisateur vers ISE (Radius)
5	ISE valide l'utilisateur sur l'AD
6	ISE retourne le résultat de l'authentification à Duo
7	Duo demande la vérification du 2FA au cloud
8	Le cloud Duo envoie un push à l'utilisateur (smartphone)
9	Le cloud retourne le résultat du 2FA au proxy Duo
10	Duo retourne le résultat d'authentification à ISE
11	ISE retourne le résultat d'authentification et d'autorisation de l'utilisateur à FTD
12	FTD accepte/refuse la connexion VPN

Démo - Flux de trafic (zoom)



Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorizati...	IP Address	Network Device
Jun 16, 2019 10:35:54.823 AM			0	francesco	8C:85:90:B6:B4:98	Macintosh...	VPN >> FTD-TO-MFA	VPN >> MFA-ALLOW-ACCESS	Employees...	10.100.255.10	
Jun 16, 2019 10:35:53.957 AM				francesco	8C:85:90:B6:B4:98		VPN >> FTD-TO-MFA	VPN >> MFA-ALLOW-ACCESS	Employees...		FTD
Jun 16, 2019 10:35:49.246 AM				francesco			VPN >> MFA-TO-ISE	VPN >> MFA-ALLOW-ACCESS	Employees...		DUO

Démo – Flux de trafic (FMC)

Edit Connection Profile

Connection Profile:* CERTIFICATE-PROFILE

Group Policy:* CERT-POLICY [Edit Group Policy](#)

Client Address Assignment **AAA** Aliases

Authentication

Authentication Method: AAA Only

Authentication Server: ISE (RADIUS)

Use secondary authentication

Authorization

Authorization Server: ISE (RADIUS)

Allow connection only if user exists in authorization database

Accounting

Accounting Server: ISE (RADIUS)

Advanced Settings

Authentication et autorisation de FTD vers ISE (et Duo en arrière plan)

Démo – Flux de trafic (Règles ISE)

Authentication Policy (4)

+ Status	Rule Name	Conditions	Use	Hits	Actions
⊘	AUTH-AD	DEVICE:Device Type EQUALS All Device Types#FTD	AD-HOME x v ➤ Options	0	⚙
⊙	MFA-TO-ISE 3	DEVICE:Device Type EQUALS All Device Types#MFA	AD-HOME x v ➤ Options	4	⚙
⊙	FTD-TO-MFA 2	DEVICE:Device Type EQUALS All Device Types#FTD	MFA x v ➤ Options	4	⚙
⊙	Default		DenyAccess x v ➤ Options	0	⚙

Active Directory → (points to AD-HOME in MFA-TO-ISE)

Duo Radius Proxy (Identity Source Sequence) → (points to MFA in FTD-TO-MFA)

Authorization Policy (3)

+ Status	Rule Name	Conditions	Results	Hits	Actions
			Profiles	Security Groups	
⊙	MFA-ALLOW-ACCESS 11	AD-HOME:ExternalGroups EQUALS supportlan.com/supportlan_users/VPN	⊗ PermitAccess +	Employees x v +	9 ⚙
⊙	MFA-ALLOW	DEVICE:Device Type EQUALS All Device Types#FTD	⊗ PermitAccess +	Employees x v +	0 ⚙
⊙	Default		⊗ DenyAccess +	Select from list v +	0 ⚙

Démo – Flux de trafic (Duo Security)

Config Duo Radius Proxy (authproxy.cfg)

Radius Client
(Validation
Utilisateur vers
ISE/AD)

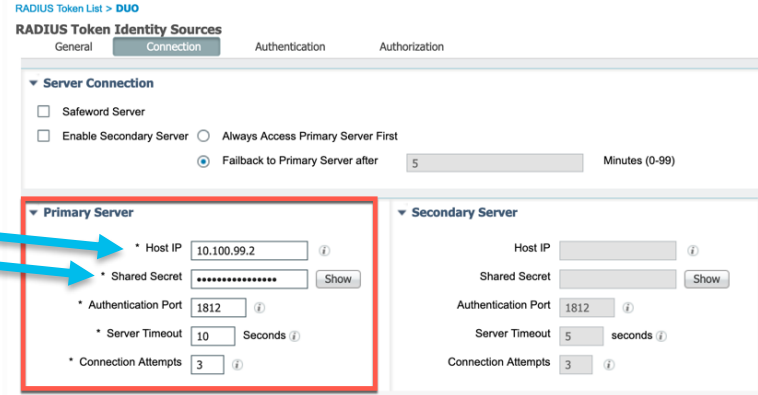
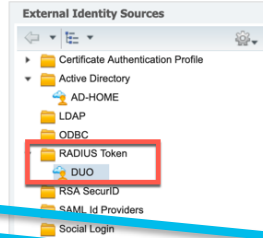
```
[radius_client]
host=10.100.99.253
secret=xxxxxxxxxx
```

Duo Cloud

```
[radius_server_auto]
ikey=xxxxxxxxxx
skey=xxxxxxxxxx
api_host=api-bc53f3f6.duosecurity.com
```

Radius Server
(Réception de la
requête
d'authentification
depuis ISE)

```
radius_ip_1=10.100.99.253
radius_secret_1=xxxxxxxxxx
radius_ip_2=10.100.254.5
radius_secret_2=xxxxxxxxxx
client=radius_client
pass_through_all=true
port=1812
failmode=safe
```



Logs Duo Radius Proxy (authproxy.log)

```
:54:58-0400 [DuoForwardServer (UDP)] Received new request id 5 from ('10.100.99.253', 47607)
:54:58-0400 [DuoForwardServer (UDP)] (('10.100.99.253', 47607), 5): login attempt for username u'francesco'
:54:58-0400 [DuoForwardServer (UDP)] Sending request for user u'francesco' to ('10.100.99.253', 1812) with id 142
:54:58-0400 [RadiusClient (UDP)] Got response for id 142 from ('10.100.99.253', 1812); code 2
:54:58-0400 [RadiusClient (UDP)] http POST to https://api-bc53f3f6.duosecurity.com:443/rest/v1/preauth
:54:58-0400 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Starting factory <_DuoHTTPClientFactory: https://api-bc53f3f6.duosecurity.com:443/rest/v1/preauth>
:54:58-0400 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.100.99.253', 47607), 5): Got preauth result for: u'auth'
:54:58-0400 [HTTPPageGetter (TLSMemoryBIOProtocol),client] Invalid ip. Ip was None
:54:58-0400 [HTTPPageGetter (TLSMemoryBIOProtocol),client] http POST to https://api-bc53f3f6.duosecurity.com:443/rest/v1/auth
:54:58-0400 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Starting factory <_DuoHTTPClientFactory: https://api-bc53f3f6.duosecurity.com:443/rest/v1/auth>
:54:58-0400 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Stopping factory <_DuoHTTPClientFactory: https://api-bc53f3f6.duosecurity.com:443/rest/v1/preauth>
:55:06-0400 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.100.99.253', 47607), 5): Duo authentication returned 'allow': 'Success. Logging you in...'
:55:06-0400 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.100.99.253', 47607), 5): Returning response code 2: AccessAccept
:55:06-0400 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.100.99.253', 47607), 5): Sending response
:55:06-0400 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Stopping factory <_DuoHTTPClientFactory: https://api-bc53f3f6.duosecurity.com:443/rest/v1/auth>
```

Dissipez vos
doutes



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

Merci pour votre participation !



La communauté est disponible dans d'autres langues

Si vous parlez anglais, espagnol, portugais, russe, chinois ou japonais, vous pouvez participer aussi dans les autres communautés Cisco.

[Cisco Community](#)

Anglais

[Сообщество Cisco](#)

Russe

[Comunidad de Cisco](#)

Espagnol

[Comunidade da Cisco](#)

Portugais

[思科服务支持社区](#)

Chinois

[シスココミュニティ](#)

Japonais

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.



