Configurer les noms de domaine UTF-8 (IDN) dans 14.X

Contenu

Introduction

Ce document décrit comment configurer et utiliser la nouvelle fonctionnalité IDN (International Domain Name) UTF-8 ajoutée à Secure Email Gateway (ESA) et à Secure Email Cloud Gateway (CES) dans le code 14.x

Contribué par Anvitha Prabhu et Libin Varghese, ingénieur TAC Cisco.

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

Concepts et configuration ESA

Components Used

Les informations de ce document sont basées sur AsyncOS pour ESA 14.0 et versions ultérieures.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Langues prises en charge dans 14.x pour la prise en charge IDN

Langues régionales indiennes

Hindi, tamoul, Telugu, Kannada, Marati, le Punjabi, le Malayalam, le Bengali, Gujarati, ourdou, Assamais, népalais, Bangla, Bodo, Dogri, Cachemire, Konkani, Maithili, Manipuri, Oriya, Sanskrit, Santali, Sindhi, Tulu.

Langues européennes/asiatiques

Allemand, français, russe, japonais, ukrainien, coréen, espagnol, italien, chinois, néerlandais, thaï, arabe, kazakh

Formats pris en charge par IDN

- Domaine IDN complet : अ न अ न् मे वि ता@जी ., @.
- Domaine IDN partiel : .को म, ಯು ಹ.ಜಿ
- ASCII, combinaison IDN : test@जी मे ल.को म

Où est prise en charge IDN ?

Routes SMTP

Accédez à Réseau -> Routes SMTP -> **Add Route** -> **Add the IDN domain** -> **Submit** -> **Commit**

Domaines DNS

Nous pouvons ajouter ou modifier des domaines IDN dans des serveurs DNS.

Accédez à Réseau -> DNS -> Modifier les paramètres -> **Ajoutez** le **domaine** IDN sous **"remplacements de serveur DNS secondaire"**

NOTE:

·les domaines IDN publics sont résolus par le serveur DNS racine public/Internet.

Domaines IDN locaux · : Dans le serveur DNS local, créez des fichiers de zone avec des enregistrements au format code postal équivalent aux domaines IDN [ex : xn—2scrj9c.xn—2scrj9c.] pour gérer la résolution des noms de domaine IDN locaux.

Écouteur - RAT/HAT

Nous pouvons utiliser la prise en charge IDN dans :

- Écouteurs entrants/sortants -> Ajouter/modifier des domaines IDN dans le domaine par défaut
- HAT/RAT ->Ajouter/modifier des domaines IDN dans HAT/RAT
- Importer/exporter des tables HAT/RAT avec IDN

Pour configurer la table d'accès aux destinataires (**RAT**) avec IDN, accédez à **Politiques de messagerie** -> **Table d'accès aux destinataires (RAT)** et cliquez sur **Ajouter un destinataire -> Ajouter le domaine IDN -> Envoyer -> Valider**

Recipient Access Table Overview

Success — Recipient Access Table entry for "जीमेल.कोम" was added.

Mode —**Cluster: ESA_BETA_CLUSTER**

▷ Centralized Management Options

Overview for Listener: Incoming   Items per page 20

Add Recipient...   Clear All Entries   Import RAT...

Order	Recipient Address	Default Action	All Delete
1	humaaralab.com	Accept	☐
2	doosralab.com	Accept	☐
3	जीमेल.कोम	Accept	☐
	All Other Recipients	Reject	

Edit Order...   Export RAT...   Delete

Pour configurer les groupes d'expéditeurs de la table d'accès hôte (HAT) avec des domaines IDN, accédez à Politiques de messagerie -> Vue d'ensemble de HAT -> Ajouter un nouveau groupe d'expéditeurs -> **Soumettre et ajouter des expéditeurs** avec le nom d'hôte IDN -> **Soumettre** ->

Sender Group: IDN_Support - Incoming

Success — Sender "जीमेल.कोम" was added.

Mode —**Cluster: ESA_BETA_CLUSTER**

▷ Centralized Management Options

Sender Group Settings

Name:	IDN_Support
Order:	9
Comment:	IDN Support
Policy:	ACCEPTED
SBRS (Optional):	Not in use
External Threat Feed (Optional): *For IP lookups only*	None
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

<< Back to HAT Overview   Edit Settings...

Find Senders

Find Senders that Contain this Text: ⑦   Find

Sender List: Display All Items in List   Items per page 20

Add Sender...

Sender	Comment	All Delete
जीमेल.कोम	idn sender	☐

<< Back to HAT Overview   Delete

NOTE: Vous pouvez suivre le même processus pour modifier n'importe quel groupe d'expéditeurs

et ajouter les domaines IDN.

Politiques de courrier entrant/sortant - Expéditeur/Récepteurs

Pour configurer les stratégies de messagerie entrante pour gérer IDN, accédez à **Politiques de messagerie** -> **Ajouter une stratégie** -> Fournir un nom de stratégie -> **Ajouter des utilisateurs**

Vous pouvez choisir d'utiliser des domaines IDN à la fois dans l'expéditeur/le destinataire ou essayer n'importe quelle combinaison ->Soumettre ->Valider

Incoming Mail Policies

Mode —**Cluster: ESA_BETA_CLUSTER**

Change Mode... ▾

▸ Centralized Management Options

Add User

○ Any Sender

◉ Following Senders

○ Following Senders are Not

Email Address:

@░░░░░.░░░

(e.g. user@example.com, user@, @example.com, @.example.com)

LDAP Group:

Query: LDAP.group ▾

Group: [   ] [Add Group] [Remove]

| |
| |

○ Any Recipient

◉ Following Recipients

░░░░@░░░░░.░░░░

(e.g. user@example.com, user@, @example.com, @.example.com)

☐ Cisco Security Awareness not configured.

LDAP Group:

Query: LDAP.group ▾

Group: [   ] [Add Group] [Remove]

| |
| |

☐ Following Recipients are Not

Email Address:

| |

(e.g. user@example.com, user@, @example.com, @.example.com)

LDAP Group:

Query: LDAP.group ▾

Group: [   ] [Add Group] [Remove]

| |
| |

[Cancel]   [OK]

NOTE: Vous pouvez suivre le même processus pour les stratégies de messages sortants.

Table des exceptions

Pour ajouter des noms de domaine IDN à la table des exceptions, accédez à

Stratégie de messagerie -> Table d'exceptions -> Ajouter une exception de vérification de l'expéditeur -> Ajouter les domaines IDN -> Envoyer -> Valider

Listes d'adresses

Pour ajouter des noms de domaine IDN à la liste d'adresses, accédez à

Politique de messagerie -> Liste d'adresses -> Ajouter une liste d'adresses -> Entrez les domaines IDN dans la zone -> Soumettre -> Commit

Address Lists

Mode —**Cluster: ESA_BETA_CLUSTER**   Change Mode...

▷ Centralized Management Options

Address Lists

Add Address List...

Address List Name	Description	Used for	Addresses	All Delete
IDN-Support	IDN-Support-test		(3) ಅನ್ನೂತಾ@ಯಾಹೂ.ಹೊತ, @जीमेल.कोम,...	☐

Delete

Contrôles de destination

Pour ajouter des noms de domaine IDN au contrôle de destination, accédez à

Politiques de messagerie -> Contrôles de destination -> **Ajouter une destination** -> Vous pouvez **ajouter le nom de domaine IDN** -> **Envoyer** -> **Valider**

| 🏠 | Monitor | Mail Policies | Security Services | Network | System Administration |

Add Destination Controls

Mode —**Cluster: ESA_BETA_CLUSTER**   Change Mode...

▷ Centralized Management Options

Destination Controls

Destination:	जीमेल.कोम
IP Address Preference:	Default (IPv6 Preferred)
Limits:	**Concurrent Connections:** ○ Use Default (500) ● Maximum of 500 (between 1 and 1,000)
	Maximum Messages Per Connection: ○ Use Default (50) ● Maximum of 50 (between 1 and 1,000)
	Recipients: ● Use Default (No Limit) ○ Maximum of 0 per 60 minutes Number of recipients between 0 and 1,000,000,000 per number of minutes between 1 and 60
	Apply limits: Per Secure Email hostname: ● System Wide ○ Each Virtual Gateway (recommended if Virtual Gateways are in use)
TLS Support:	Default (None) DANE Support: ⑦ Default (None)
Bounce Verification:	Perform address tagging: ● Default (No) ○ No ○ Yes Applies only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.
Bounce Profile:	Default Bounce Profile can be configured at Network > Bounce Profiles.

Note: DANE will not be enforced for domains that have SMTP Routes configured.

Cancel   Submit

Destination Controls

Mode —**Cluster: ESA_BETA_CLUSTER**   Change Mode...

▷ Centralized Management Options

Destination Control Table   Items per page 20

Add Destination...   Import Table

Domain ▲	IP Address Preference	Destination Limits	TLS Support	DANE Support ^	Bounce Verification *	Bounce Profile	All Delete
doosralab.com	Default	Default connection limit, 50 messages per connection, Default recipient limit	Required	Default	Default	Default	☐
humaaralab.com	Default	Default connection limit, 50 messages per connection, Default recipient limit	Required	Default	Default	Default	☐
जीमेल.कोम	Default	500 concurrent connections, 50 messages per connection, Default recipient limit	Default	Default	Default	Default	☐
Default	IPv6 Preferred	500 concurrent connections, 50 messages per connection, No recipient limit	None	None	Off	Default	

Export Table   Delete

* Bounce Verification settings apply only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.
^ DANE will not be enforced for domains that have SMTP Routes configured.

Global Settings

Certificate:	Client-Cert
Send an alert when a required TLS connection fails:	Enabled

Edit Global Settings...

Profils de renvoi

Le destinataire des messages de renvoi et d'avertissement peut être configuré avec le nom de domaine IDN sous Profils de renvoi.

Accédez à **Network** -> **Bounce Profiles** -> **Add Bounce Profile** -> Enter name -> Configure the values for bounce Profile -> For Recipient for Bounce and Warning Messages -> Select **Alternate address** et vous pouvez choisir d'utiliser l'adresse de domaine IDN.

LDAP

Vous pouvez maintenant avoir les requêtes LDAP accept/group avec les noms de domaine IDN comme indiqué dans l'image.

Quarantaine du spam local

Vous pouvez voir la quarantaine SPM locale qui affiche les noms de domaine IDN dans l'adresse e-mail/domaines/objet de l'utilisateur
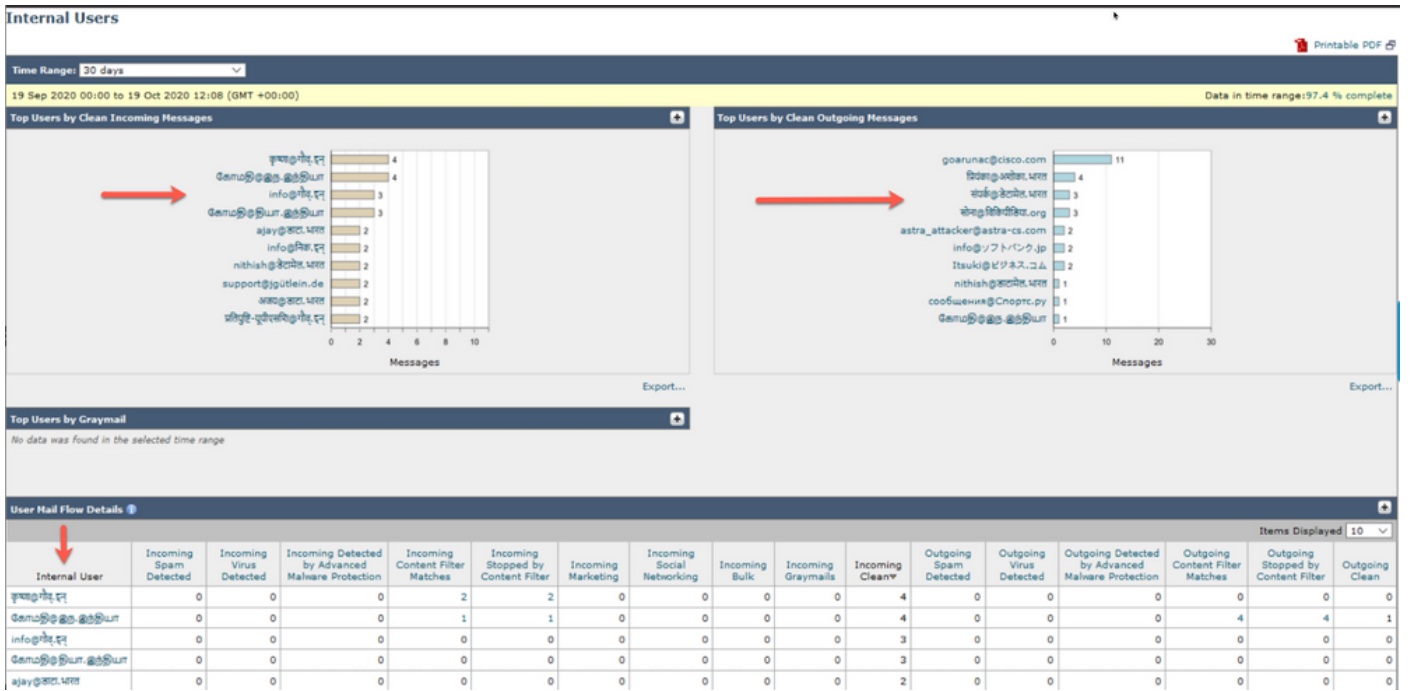
NOTE: La quarantaine PVO locale affiche un comportement similaire à celui de la quarantaine du spam.

Vérification et dépannage

1) Les rapports sur ESA et SMA (Secure Email and Web Manager) prennent désormais en charge IDN. Nous pouvons voir les noms d'utilisateur/domaine/adresse e-mail au format IDN sur les rapports

Accédez à **Surveillance** -> **Utilisateurs internes**

2) Dans **Suivi des messages**, nous pouvons voir le nom de domaine IDN et également filtrer avec les domaines IDN/noms d'utilisateurs/adresse de messagerie

3) Utilisez la commande CLI grep ou tail pour afficher "**mail_logs**" et nous voyons les domaines IDN dans les journaux

```
Mon Feb  8 21:47:11 2021 Info: Start MID 23569633 ICID 148853
Mon Feb  8 21:47:11 2021 Info: MID 23569633 ICID 148853 From:
```

<@.>

```
Mon Feb  8 21:47:19 2021 Info: MID 23569633 ICID 148853 RID 0 To: <test@lab.com>
Mon Feb  8 21:47:52 2021 Info: MID 23569633 Subject 'Please read as this is very  for both the
countries.'
Mon Feb  8 21:47:52 2021 Info: MID 23569633 SDR: Domains for which SDR is requested: reverse DNS
host: sample.host.com, helo: lab.com, env-from: ., header-from: Not Present, reply-to: Not
Present
Mon Feb  8 21:47:53 2021 Info: MID 23569633 SDR: Consolidated Sender Reputation: Tainted, Threat
Category: N/A, Suspected Domain(s) : lab.com. Youngest Domain Age: 3 months 29 days for domain:
lab.com
Mon Feb  8 21:47:53 2021 Info: MID 23569633 SDR: Tracker Header :
87dSxFfNYdSiOahrxSUZFOrdpenKiF6J2uKiPf+SFKCtj52hNCpe6LDQ8UFAliGnUDA7FsuXLvHTcaATt6AKG4PWLpwEeo/d
cIPBUOdxB48=
Mon Feb  8 21:47:53 2021 Info: MID 23569633 ready 605 bytes from
```

<@.>

```
Mon Feb  8 21:47:53 2021 Info: MID 23569633 matched all recipients for per-recipient policy
DEFAULT in the inbound table
Mon Feb  8 21:47:53 2021 Info: MID 23569633 interim verdict using engine: CASE spam positive
Mon Feb  8 21:47:53 2021 Info: MID 23569633 using engine: CASE spam positive
Mon Feb  8 21:47:53 2021 Info: ISQ: Tagging MID 23569633 for quarantine
Mon Feb  8 21:47:53 2021 Info: MID 23569633 interim AV verdict using McAfee CLEAN
Mon Feb  8 21:47:53 2021 Info: MID 23569633 interim AV verdict using Sophos CLEAN
Mon Feb  8 21:47:53 2021 Info: MID 23569633 antivirus negative
Mon Feb  8 21:47:53 2021 Info: MID 23569633 AMP file reputation verdict : SKIPPED (no attachment
in message)
Mon Feb  8 21:47:53 2021 Info: MID 23569633 using engine: GRAYMAIL negative
Mon Feb  8 21:47:53 2021 Info: MID 23569633 Custom Log Entry: SDR Age is less than 1 Year
Mon Feb  8 21:47:53 2021 Info: MID 23569633 Outbreak Filters: verdict negative
Mon Feb  8 21:47:53 2021 Info: MID 23569633 Message-ID '<d35764$mf971@esa1.lab.com>'
Mon Feb  8 21:47:53 2021 Info: MID 23569633 queued for delivery
Mon Feb  8 21:47:53 2021 Info: New SMTP DCID 250225 interface 10.0.202.17 address 10.0.201.5
port 6025
Mon Feb  8 21:47:53 2021 Info: DCID 250225 STARTTLS command not supported
Mon Feb  8 21:47:53 2021 Info: Delivery start DCID 250225 MID 23569633 to RID [0] to offbox
IronPort Spam Quarantine
Mon Feb  8 21:47:53 2021 Info: Message done DCID 250225 MID 23569633 to RID [0] (external
quarantine)
Mon Feb  8 21:47:53 2021 Info: MID 23569633 RID [0] Response 'ok:  Message 27293054 accepted'
Mon Feb  8 21:47:53 2021 Info: Message finished MID 23569633 done
Mon Feb  8 21:47:58 2021 Info: DCID 250225 close
```

Informations connexes

- [Cisco Email Security Appliance - Guides de l'utilisateur final](#)
- [Support et documentation techniques - Cisco Systems](#)