



Cisco ESA, Umbrella et WSA Sécurisation d'Emails et du Trafic Web

Community Live Webinar

Redouane Meddane

Instructeur Cisco CCSI 35458 | CCNP Security, Collaboration et Enterprise | F5 BIG-IP Administrator

15 novembre 2022

Des nouveaux sujets tous les mois

La Communauté francophone Cisco grandit

Grâce à la participation de tous nos collaborateurs, notre communauté grandit pour vous offrir des nouveaux webinaires sur différentes technologies.

Inscrivez-vous et participez !

[Prochains événements](#)

[Événements précédents](#)

[Optimisez l'accès au Cloud avec Cisco SD-WAN](#)

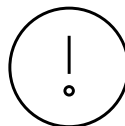
le mardi 22 novembre 2022

[Programmabilité Cisco Catalyst / IOS-XE](#)

le mardi 6 décembre (en attente de confirmation)

[Webex et le RGPD \(2022\)](#)

le mardi 13 décembre 2022



Connectez, Engagez, Collaborez !

Solutions

Acceptez les solutions qui sont correctes et complimentez ceux qui vous ont aidé ! Aidez autres utilisateurs à trouver les réponses correctes dans la fenêtre de recherche.

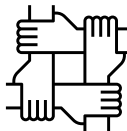
Accepter comme solution

Compliments

Mettez en évidence les autres membres. Les votes utiles motivent les membres enthousiastes en leur offrant un signe de reconnaissance !



0 Compliments



Spotlight Awards

De nouveaux lauréats tous les mois !

Démarquez-vous par vos efforts et votre engagement à améliorer la communauté et à aider les autres membres. Les [Spotlight Awards](#) sont distribués chaque mois pour mettre en valeur les membres les plus remarquables.

Maintenant vous pouvez aussi désigner un candidat ! [Cliquez ici](#)



Redouane Meddane



Présentateur

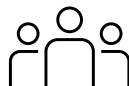
Redouane Meddane est Instructeur Cisco CCSI N°35458, il est aussi certifié en CCNP Security, CCNP Collaboration, CCNP Enterprise et F5 BIG-IP Administrator. Résident en Algérie, il est enseignant et formateur pour les certifications Cisco. Il possède un blog personnel ipdemystify.com (en anglais) où il écrit et partage des articles qui traitent sur divers sujets de protocole de routage OSPF, la sécurité et la collaboration. En plus, Redouane est également blogger dans mhd-experts.com, un blog dédié à la communauté informatique francophone avec d'autres experts.

Redouane a reçu ces Cisco Awards :

- 2019 Cisco Distinguished Instructor Award
- 2019 Cisco Security Instructor Excellence Award
- 2020 Cisco Distinguished Instructor Award
- 2020 Cisco Security Instructor Excellence Award
- 2021 Cisco Collaboration Instructor Excellence Award

Téléchargez la présentation !

<https://bit.ly/WEBsld-nov22>



Agenda



- Cisco Web Security Appliance (WSA)



- Cisco Umbrella



- Cisco Email Security Appliance (ESA)

Cisco Web Security Appliance

Introduction au Web Security Appliance WSA

Fonctionnalités

Proxy (HTTP/HTTPS/FTP)

Caching

URL Filtering (par category)

Application Visibility Control

Reputation WBRS (Web Based Reputation Score)
Block [-10 à -9], Scan [-8.9 à 5.9], allow [6 à 10].

Dynamic Content Analysis

User Authentication

Bandwidth Limits

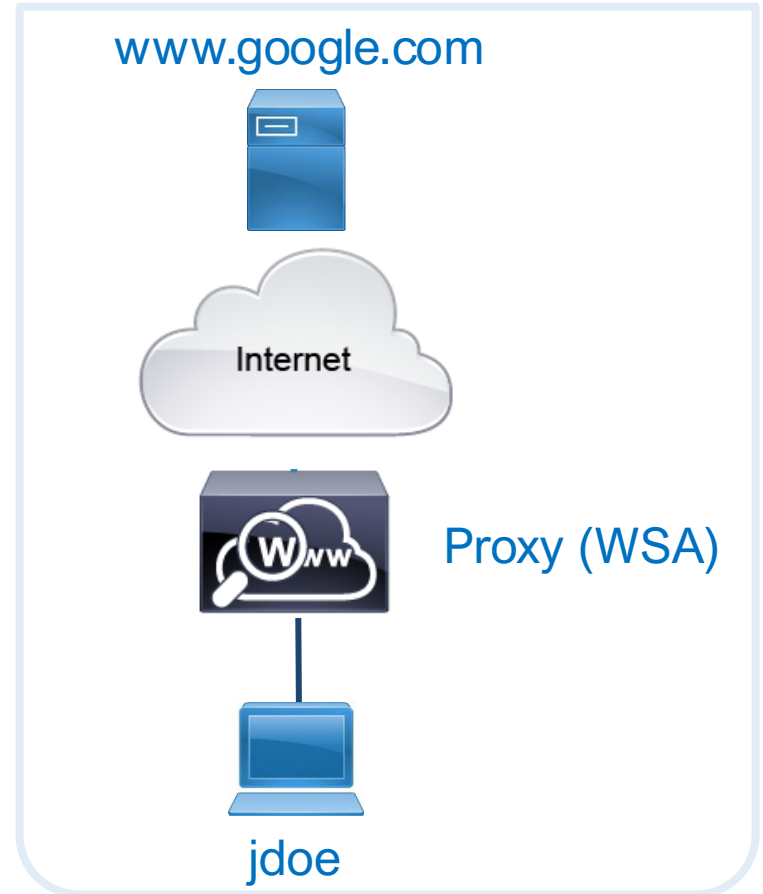
Time Quotas

File Detection

- AMP, local AV (McFee, Sophos)

SSL Decryption

L4TM L4 Traffic Monitor



WSA Plateformes et Interfaces



Plateformes

Physique

S1xx (Small), S3xx (medium), S6xx (Large)
Disque, RAM, CPU

Virtuel

S000v (Test), S100v, S300v, S600v
Disque, RAM, CPU



Interfaces

Data

-Web Proxy (P1 , P2)
-L4TM (T1 , T2)

Administration

-Management M1 (HTTP,
HTTPS et SSH)

Mode de déploiement

Deux modes de proxy avec une option L4TM service

- Modes Proxy
 - Explicit Forward
 - Transparent
- L4TM (Layer 4 Traffic Monitor)
 - Trafic copié vers l'interface T1 ou T2 en utilisant le SPAN. Similaire à un IDS. « Détecte les malwares au niveau d'un trafic non-http et non-https »

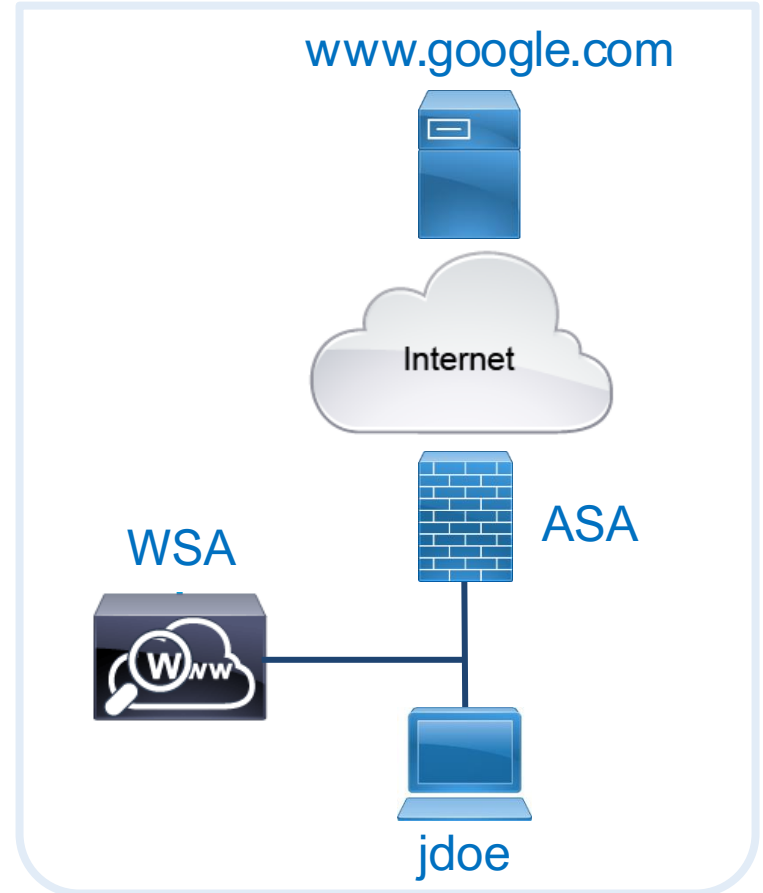
Explicit Forward Mode

Le trafic web est envoyé directement au WSA

- Manuel: paramètres proxy du navigateur
- Automatique: PAC file

Considérations

- La résolution DNS par le WSA
- IP de destination = WSA



WSA Policies



Requête Web

Identification Profile

Conditions:

- Subnet
- Protocol
- Port
- User Agent

Résultat

- Authentication
- Pas authentication

Access Policy

Conditions:

- Identification Profile
- user/AD Group

Filtres

- Protocol/User Agent
- URL Filtering
- Applications
- Objects (File Type)
- Anti-Malware/Réputation

Action

- ✓ Block, Monitor, Warn,
- ✓ Quota Based, Time Based,
- ✓ Bandwidth Limit (application)

Decryption Policy

Conditions:

- Identification Profile
- user/AD Group

Filtres

- URL Filtering
- WBRS

Action

- ✓ Decrypt
- ✓ Passthrough
- ✓ Drop
- ✓ Monitor

Polling Question 1

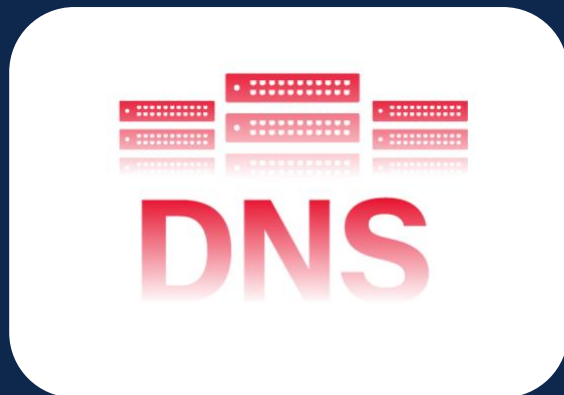
En mode Explicit Forward, quelle est l'entité qui fait la résolution DNS ?

- 1) Client
- 2) WSA
- 3) Firewall

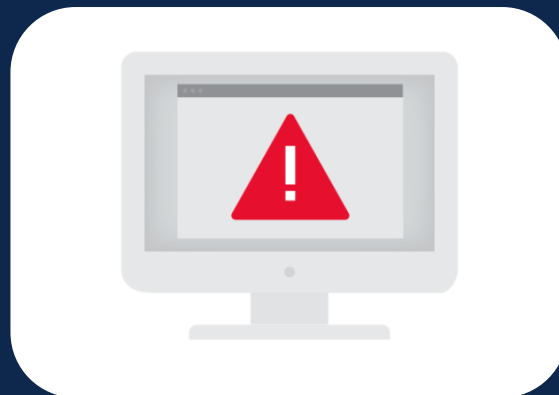
Cisco Umbrella

L'importance du DNS

D'après l'équipe de recherche en sécurité de Cisco



91.3% des attaques malware
utilisent DNS



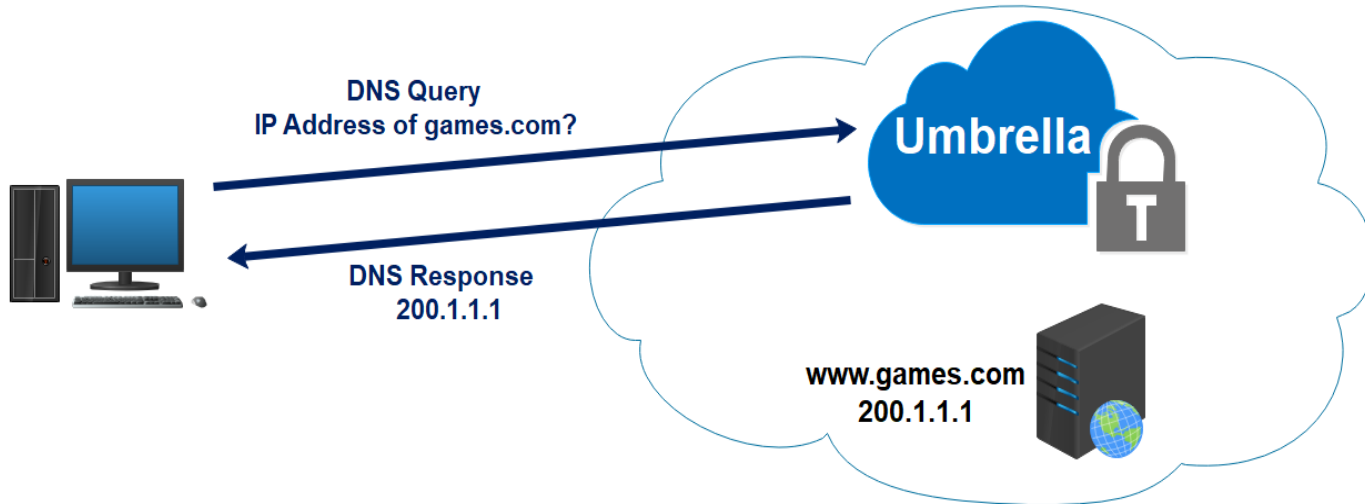
68% des organisation n'inspecte pas
le trafic DNS.

Umbrella comme service DNS

Tout commence par le DNS.

Umbrella est un service DNS.

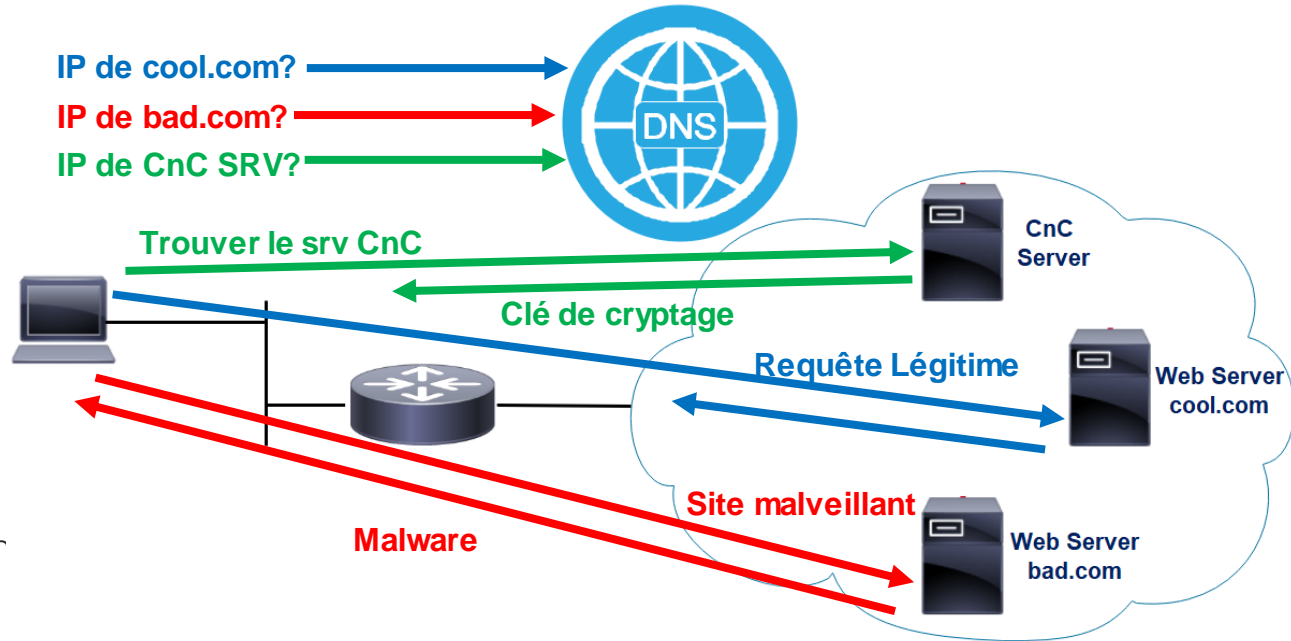
Le DNS précède l'exécution du fichier et la connexion IP.



Attaque Ransomware

Le dilemme d'un attaquant

1. Comment rediriger vers un serveur malveillant?
2. Comment contacter un serveur CnC?
3. Que va-t-il faire avec un host infecté?



Umbrella n'est pas qu'un service DNS

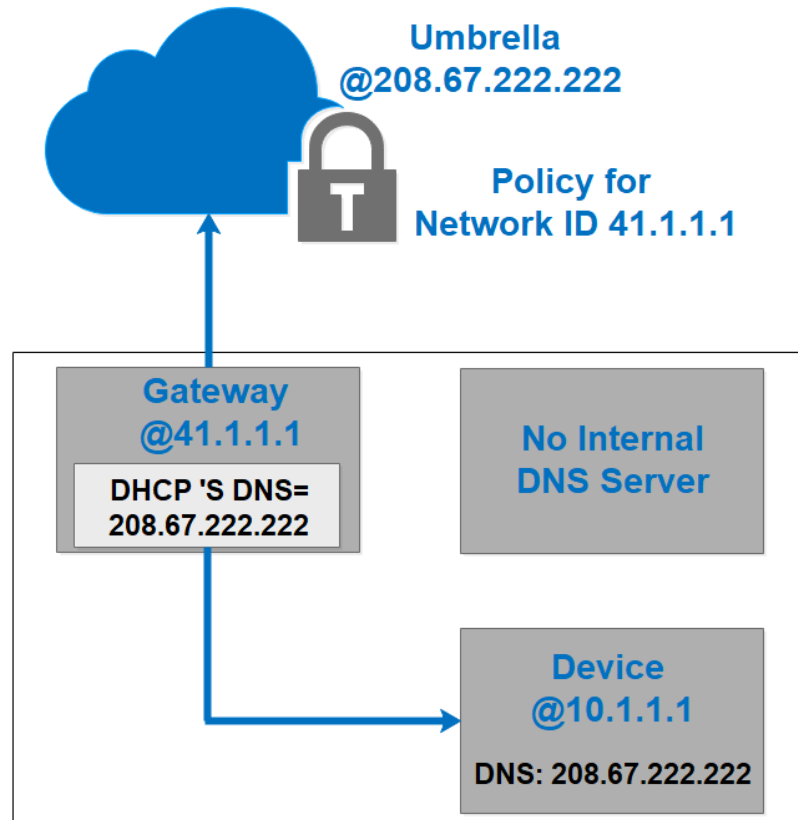
- Threat Prevention
- Protection On & Off Network
- Block par Domains, IPs & URLs
- Proxy et inspection des fichiers (Intelligent proxy, SSL Decryption)

Déploiement sans serveur DNS interne

- Le serveur DNS des PC c'est Umbrella tout court.

Considérations

La seule visibilité est l'adresse publique des utilisateurs. Conséquence une seule policy pour tout le monde.

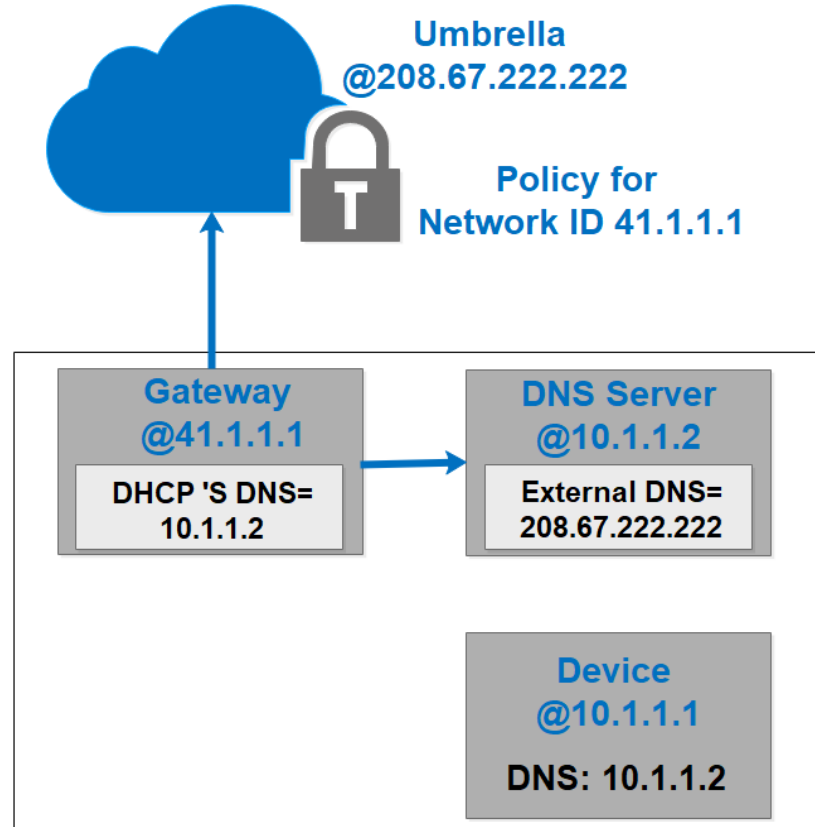


Déploiement avec serveur DNS interne

- Le serveur DNS interne route les requêtes DNS externes (Les forwarders) vers Umbrella

Considérations

La seule visibilité est l'adresse publique des utilisateurs. Conséquence une seule policy pour tout le monde.

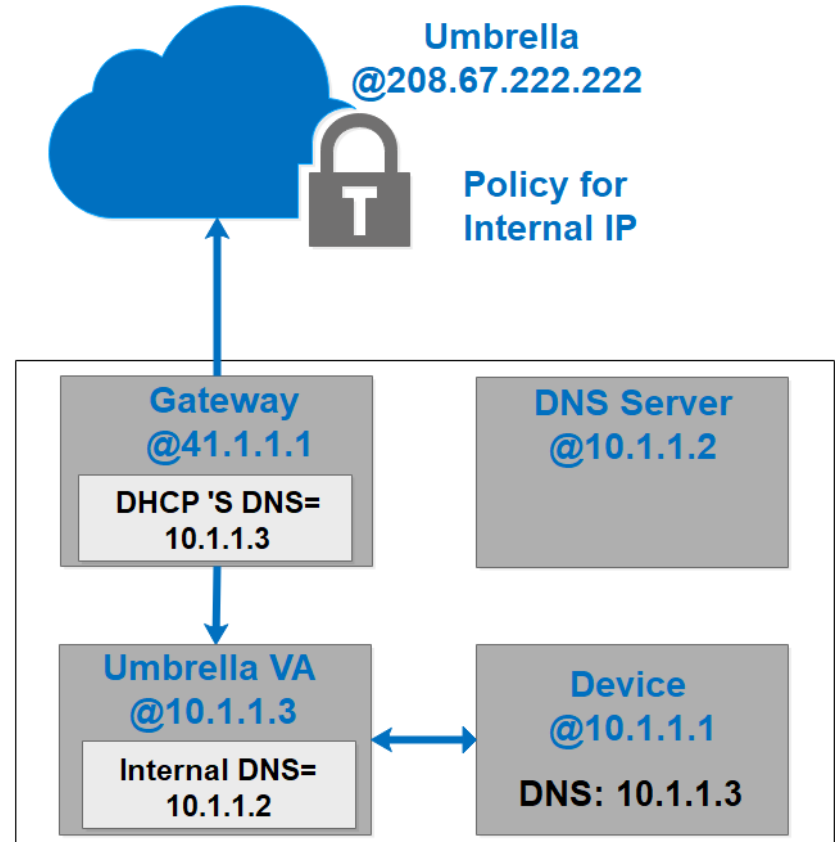


Déploiement avec une appliance virtuelle Umbrella VA

- Virtual Appliance Umbrella (VA) est le serveur DNS des users.
- Les résolutions DNS internes et externes passent par la VA
- La VA ajoute l'IP interne host dans les requêtes DNS.

Considérations

Policy basée sur l'adresse IP interne. Plus de granularité.

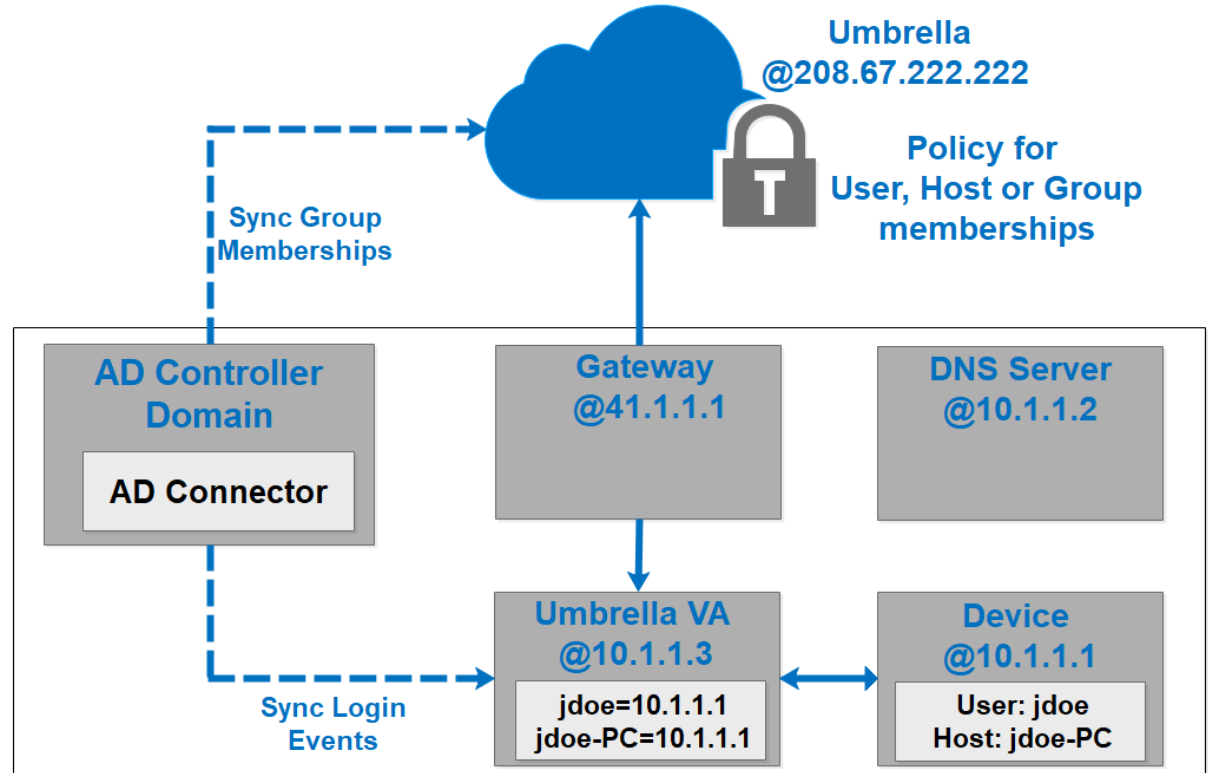


Déploiement avec une VA Umbrella et Active Directory

- Synchronisation des groupes AD/Users AD avec Umbrella

Considérations

Des politiques basées sur les groupes AD/Users AD.



Déploiement avec un client Umbrella

- Protection OFF-Network (Télétravail) et On-Network.
- Un client Umbrella installé dans le PC, les requêtes DNS sont redirigées vers Umbrella.

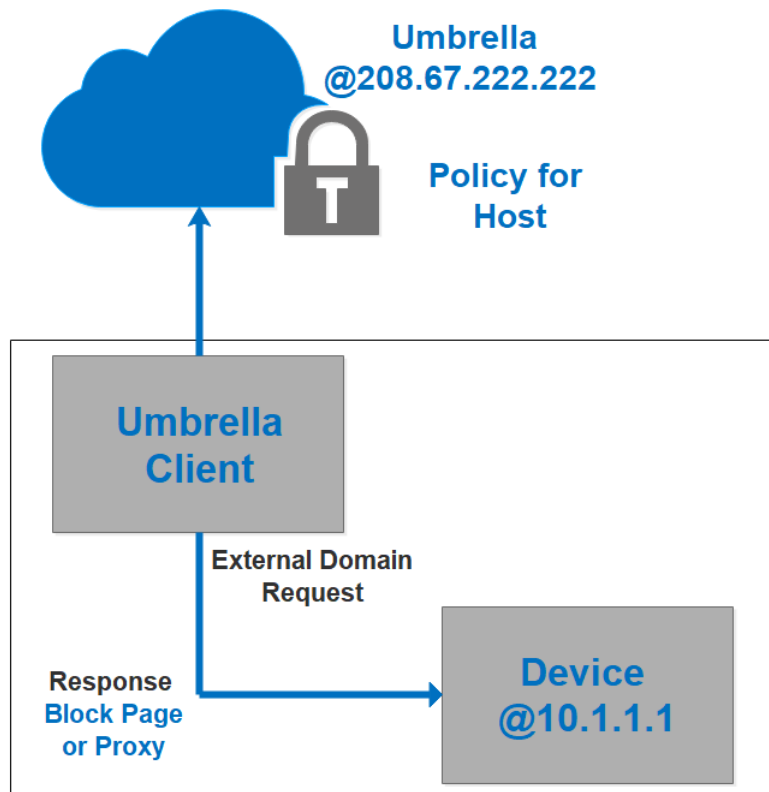
Considérations

Des politiques basées sur le nom des machines.

Deux clients:

Umbrella Roaming Client



Roaming Security AnyConnect Module.



Client Umbrella



Umbrella Roaming Client (2.2.356.0)

IPv4 DNS status:

-  Protected
-  Encrypted


User Identity:
IPv4 Address: 10.254.253.120

IPv6 DNS status (BETA):

-  Not Required
-  Unencrypted

User Identity:
IPv6 Address:

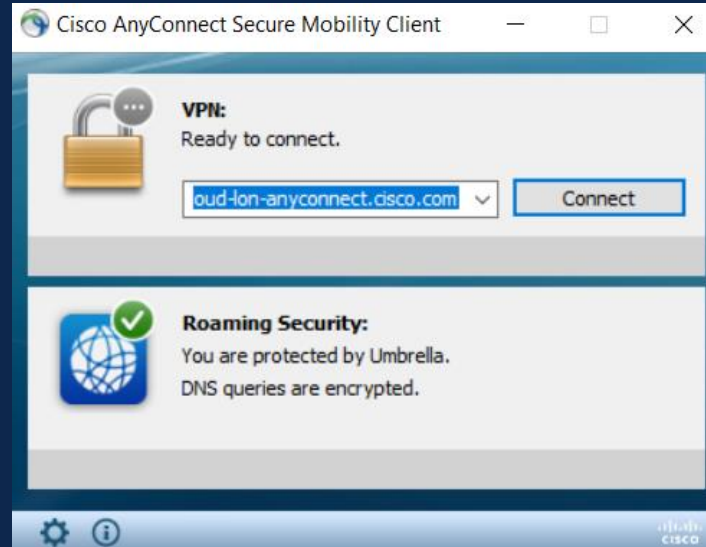
IP Layer Enforcement status:

-  Disabled

Details:


Last Connected: 35 min ago
Logging: Off
Client Name: Redouane
Organization Id: 3050180
Device Id: 010174809F5C3355

[Run Diagnostic Tool](#)



The screenshot shows the Cisco AnyConnect Secure Mobility Client window. The title bar reads "Cisco AnyConnect Secure Mobility Client". The main content area is divided into two sections. The top section, titled "VPN:", shows a yellow padlock icon and the text "Ready to connect.". Below this is a dropdown menu with the text "oud-lon-anyconnect.cisco.com" and a "Connect" button. The bottom section, titled "Roaming Security:", shows a blue globe icon with a green checkmark and the text "You are protected by Umbrella. DNS queries are encrypted.". At the bottom of the window, there are icons for settings and information, and the Cisco logo.

A la découverte de l'interface graphique

 Redouane Protected & Encrypted at the DNS Layer 42 minutes ago

✔ Layer
DNS Layer Encryption: enabled

Roaming Computer Information

Identity Name [↗](#)
Redouane

Hostname Redouane	Original Hostname DESKTOP-12255ED
----------------------	--------------------------------------

OS Version Windows 10	Client Type Umbrella RC Version: 2.2.356	Last Synced 42 minutes ago
--------------------------	---	-------------------------------

Security Information

Status ✔ Protected	DNS Layer Security 🔒 Yes	IP Layer Enforcement ✔ Disabled	Last Active Policy 🛡️ Demo-Policy
------------------------------------	--	------------------------------------	---

Tags:
[+ ADD TAG](#)

[DELETE](#) [CLOSE](#)

Policies

← → ↻ 🏠 🔒 https://dashboard.umbrella.com/o/3050180/#/policies/management/policies 🔍 📄 🌐

Cisco Umbrella **Free Trial:** You have 13 days left. [VIEW PRICING & PURCHASE](#)

Deployments >
Policies >
Management
All Policies
Policy Components
Destination Lists
Content Categories
Application Settings
Security Settings
Block Page Appearance
Integrations
Reporting >
Admin >
Investigate

Policies / Management
All Policies ⓘ

[+](#) Add [⚙️](#) Policy Tester

Policies dictate the security protection, category settings, and individual destination lists you can apply to some or all of your identities. Policies also control log levels and how block pages are displayed. Policies are enforced in a descending order, so your top policy will be applied before the second if they share the same identity. To change the priority of your policies, simply drag and drop the policy in the order you'd like. More policy info can be found in [this article](#).

Sorted by Order of Enforcement

1	Default Policy	Applied To All Identities	Contains 3 Policy Settings	Last Modified Mar 16, 2020	⌵
---	----------------	------------------------------	-------------------------------	-------------------------------	---

Création d'une policy - Conditions

The screenshot shows the Cisco Umbrella dashboard interface. On the left is a dark sidebar with navigation options: Deployments, Policies, Management (highlighted), All Policies, Policy Components (Destination Lists, Content Categories, Application Settings, Security Settings, Block Page Appearance, Integrations), Reporting, Admin, and Investigate. The main content area is titled "What would you like to protect?". It features a "Select Identities" section with a search box and a list of "All Identities" including AD Groups, AD Users, AD Computers, Networks, Roaming Computers (2 >), Sites (1 >), Network Devices, Mobile Devices, and Chromebooks. To the right is a dashed box labeled "0 Selected". At the bottom right of the main area are "CANCEL" and "NEXT" buttons. The bottom right corner of the dashboard indicates "Sorted by Order of Enforcement".

Création d'une policy - Filtres

https://dashboard.umbrella.com/o/3050180/#/policies/management/policies

Policies / Management
All Policies

Add Policy Tester

Policies dictate the security protection, category settings, and individual destination lists you can apply to some or all of your identities. Policies also control log levels and how block pages are displayed. Policies are enforced in a descending order, so your top policy will be applied before the second if they share the same identity. To change the priority of your policies, simply drag and drop the policy in the order you'd like. More policy info can be found in [this article](#).

What should this policy do?
Choose the policy components that you'd like to enable.

- Enforce Security at the DNS Layer**
Ensure domains are blocked when they host malware, command and control, phishing, and more.
- Inspect Files**
Selectively inspect files for malicious content using antivirus signatures and Cisco Advanced Malware Protection.
- Limit Content Access**
Block or allow sites based on their content, such as file sharing, gambling, or blogging.
- Control Applications**
Block or allow applications and application groups for identities using this policy.
- Apply Destination Lists**
Lists of destinations that can be explicitly blocked or allowed for any identities using this policy.

▶ **Advanced Settings**

CANCEL PREVIOUS NEXT

Création d'une policy – Block Page

The screenshot shows the Cisco Umbrella dashboard interface. On the left is a dark sidebar with navigation options: Overview, Deployments, Policies, Management (highlighted), All Policies, Policy Components (Destination Lists, Content Categories, Application Settings, Security Settings, Block Page Appearance, Integrations), Reporting, Admin, and Investigate. The main content area is titled 'Set Block Page Settings' and includes instructions to 'Define the appearance and bypass options for your block pages.' There are three steps in a progress bar: 'Content' (checked), 'Block Pages' (active), and 'Summary' (starred). The 'Block Pages' section has two radio button options: 'Use Umbrella's Default Appearance' (selected) with a 'Preview Block Page' link, and 'Use a Custom Appearance' with a dropdown menu labeled 'Choose an existing appearance'. Below these are expandable sections for 'BYPASS USERS' and 'BYPASS CODES'. At the bottom right of the form are 'CANCEL', 'PREVIOUS', and 'NEXT' buttons. Below the form is a table with the following data:

	Applied To	Contains	Last Modified	
1 Default Policy	All Identities	3 Policy Settings	Mar 16, 2020	▼

Création d'une policy – Intelligent Proxy

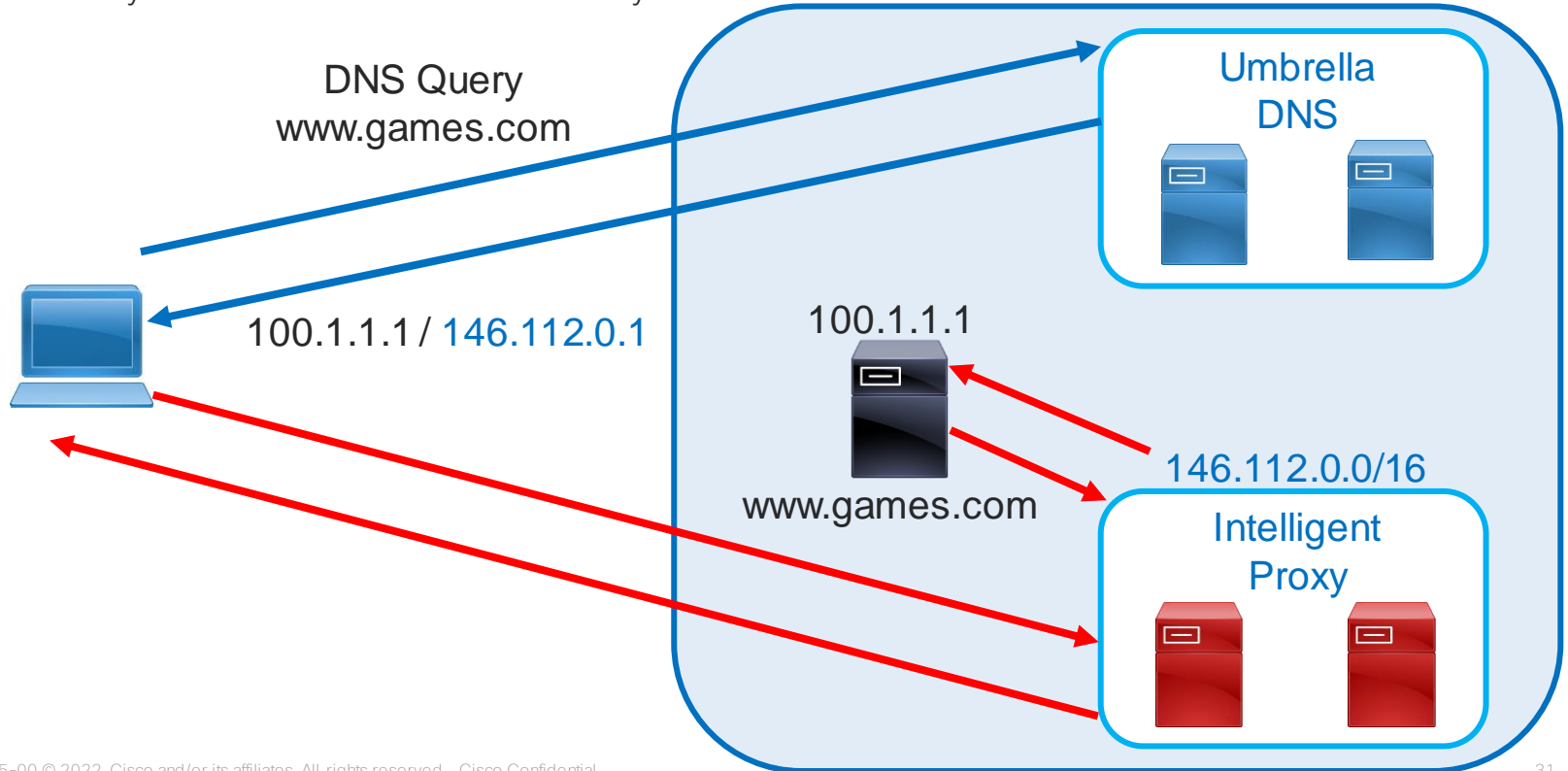
The screenshot displays the Cisco Umbrella dashboard interface. On the left is a dark sidebar with navigation options: Overview, Deployments, Policies, Management (highlighted), Policy Components (All Policies, Destination Lists, Content Categories, Application Settings, Security Settings, Block Page Appearance, Integrations), Reporting, Admin, Investigate, and a user profile for Redouane MEDDANE. The main content area shows the 'Policy Summary' for a policy named 'Demo-Policy'. At the top, there are three tabs: 'Content', 'Block Pages', and 'Summary' (which is active). The summary includes several status items:

- Policy Name:** Demo-Policy
- 1 Identity Affected:** 1 Roaming Computer (with an [Edit](#) link)
- 0 Destination List Enforced:** 1 Block List (with an [Enable](#) link)
- No Security Settings Applied:** (with an [Enable](#) link)
- File Analysis Not Enabled:** File Inspection Not Enabled (with an [Edit](#) link)
- Content Setting Applied: Default Settings:** Games, Social Networking, File Transfer Services, plus 1 more will be blocked. (with [Edit](#) and [Disable](#) links)
- Umbrella Default Block Page Applied:** (with [Edit](#) and [Preview Block Page](#) links)
- No Application Settings Applied:** (with an [Enable](#) link)

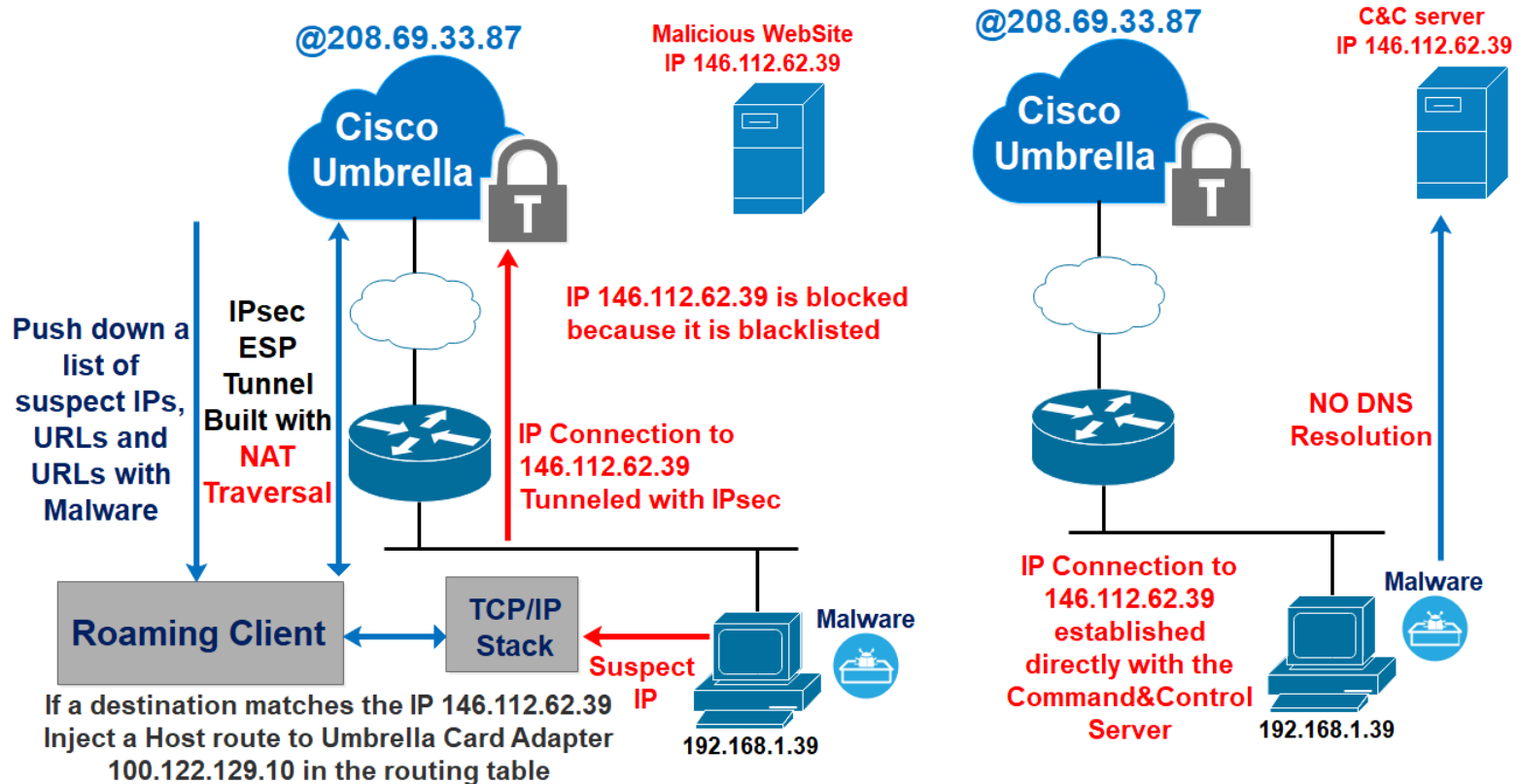
At the bottom right of the summary area, there are three buttons: 'CANCEL', 'PREVIOUS', and 'SAVE'. Below the summary is a section for 'Advanced Settings' with a right-pointing arrow.

Intelligent Proxy

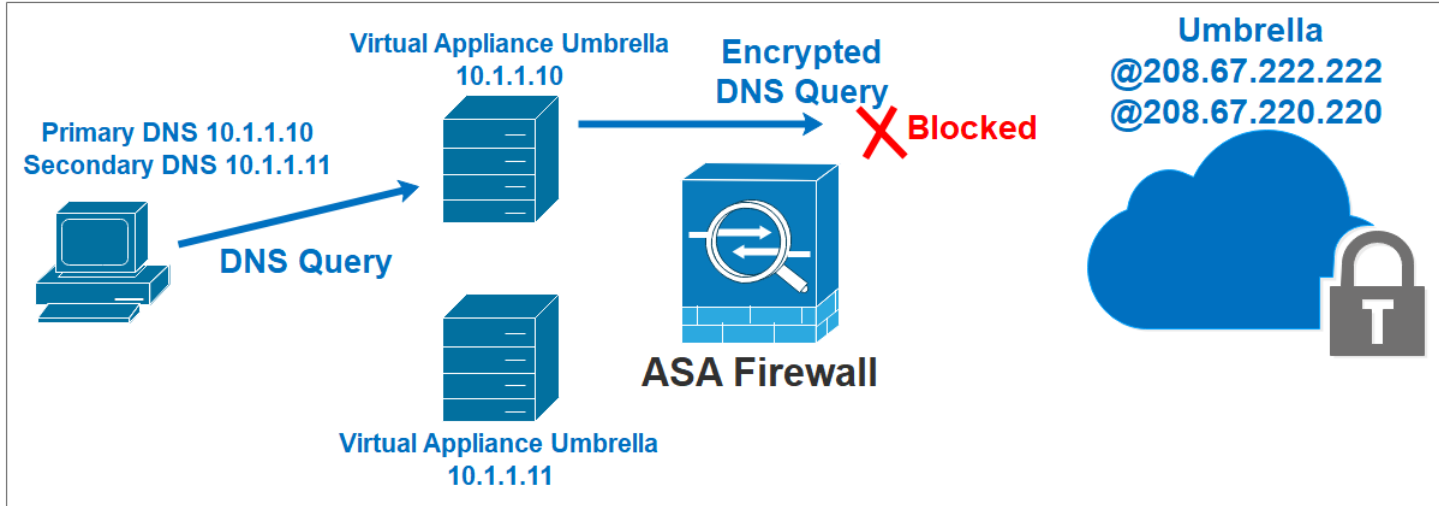
Intelligent Proxy = Cisco Cloud Web Security



IP Layer Enforcement



Use case



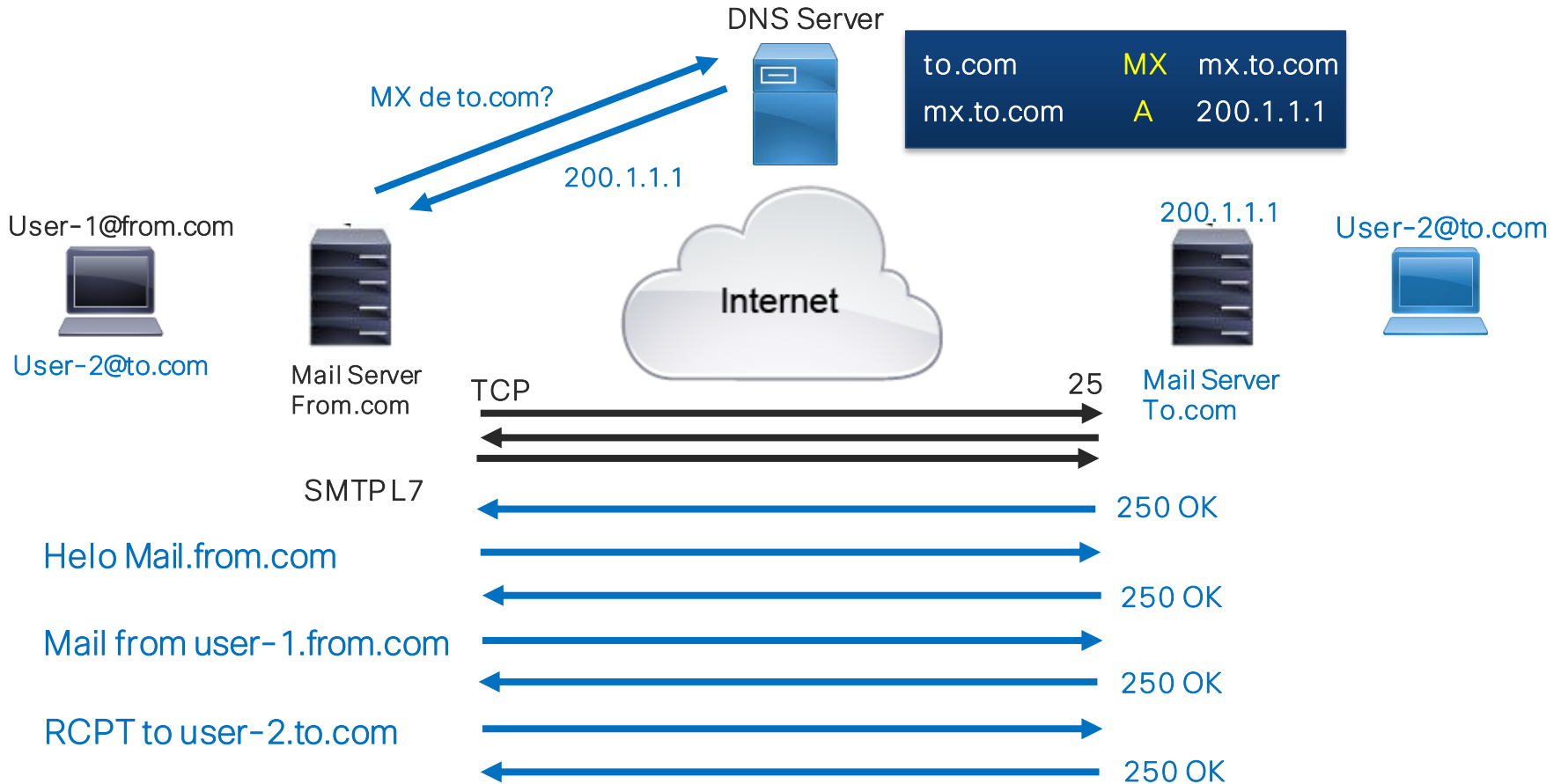
Polling Question 2

La fonctionnalité IP Layer Enforcement permet de se prémunir contre quel type de bypass?

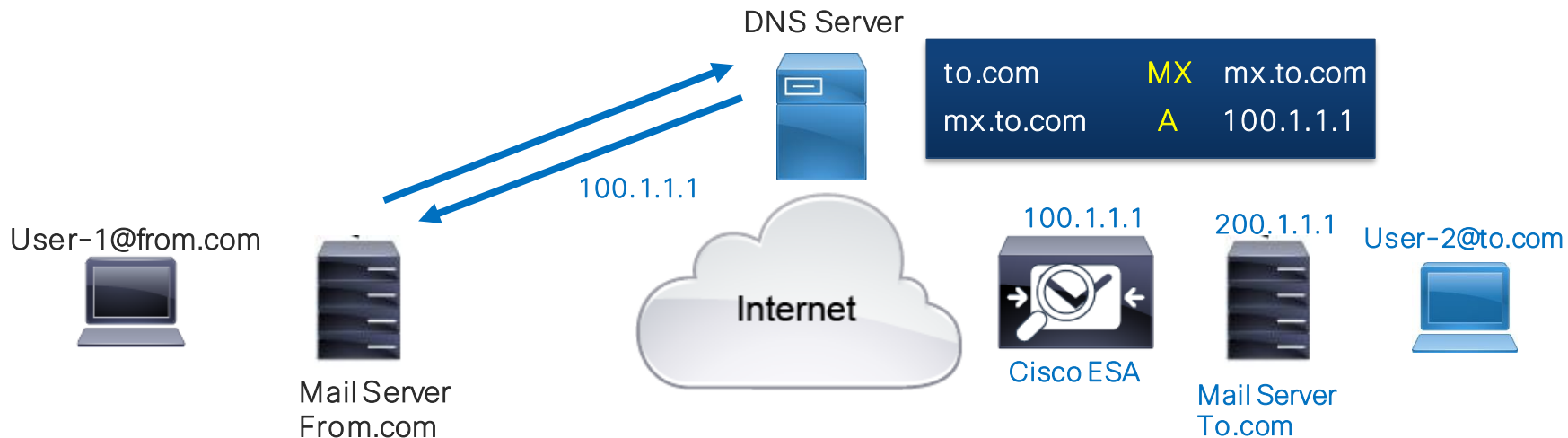
- 1) Bypasser les firewalls Edge
- 2) Bypasser la couche Security DNS
- 3) Bypasser le proxy Umbrella (Intelligent Proxy)

Cisco Email Security Appliance

Comment SMTP fonctionne



Comment SMTP fonctionne



Listeners HAT RAT

Cisco ESA se base sur des listeners.

Les listeners sont des services SMTP qui fonctionnent au niveau de l'interface.

Public: Listener pour les mail entrants

Private: Listener pour les mails sortants.

Les listeners se basent sur deux tables:

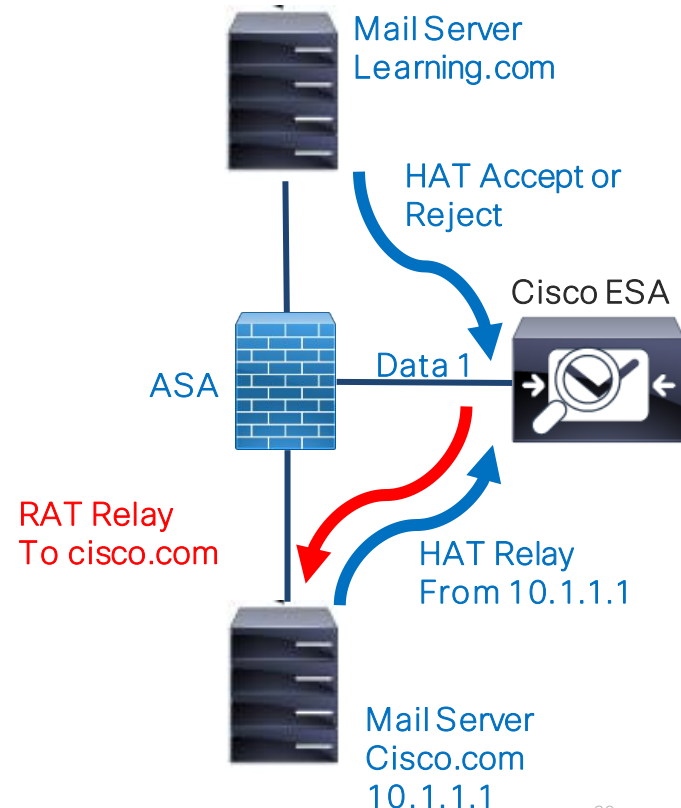
HAT: Host Access Table

RAT: Recipient Access Table

Mais quel est le rôle du HAT et du RAT?

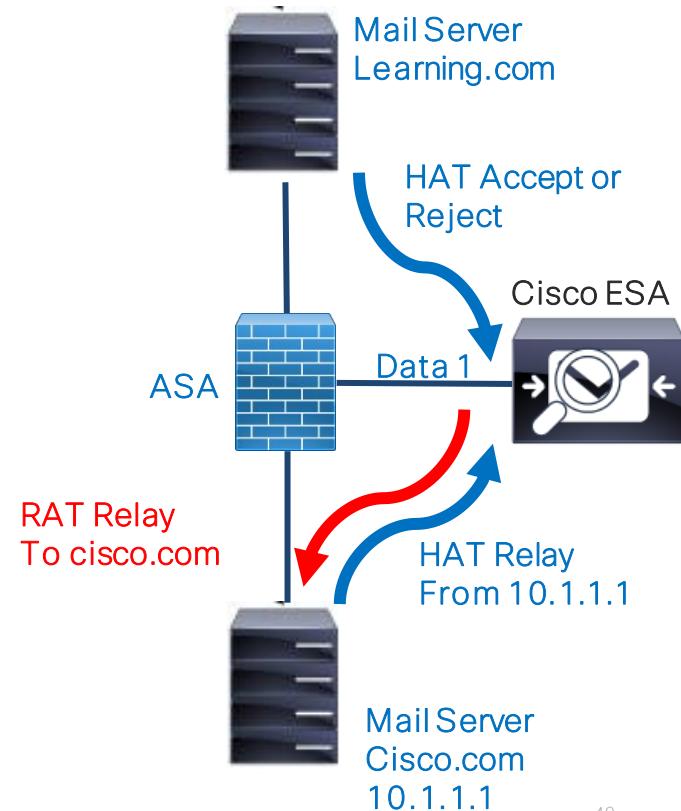
Listeners HAT RAT

- **Public listener (Incoming mail)**: Nous avons besoin du **HAT** et du **RAT**. **HAT** pour vérifier le sender et le **RAT** pour vérifier le recipient **destiné** a notre **domaine interne**.
- **Private listener (Outgoing mail)**: Nous avons besoin du **HAT** seulement pour relayer les mails sortants **émanant** de notre **serveur SMTP interne**.

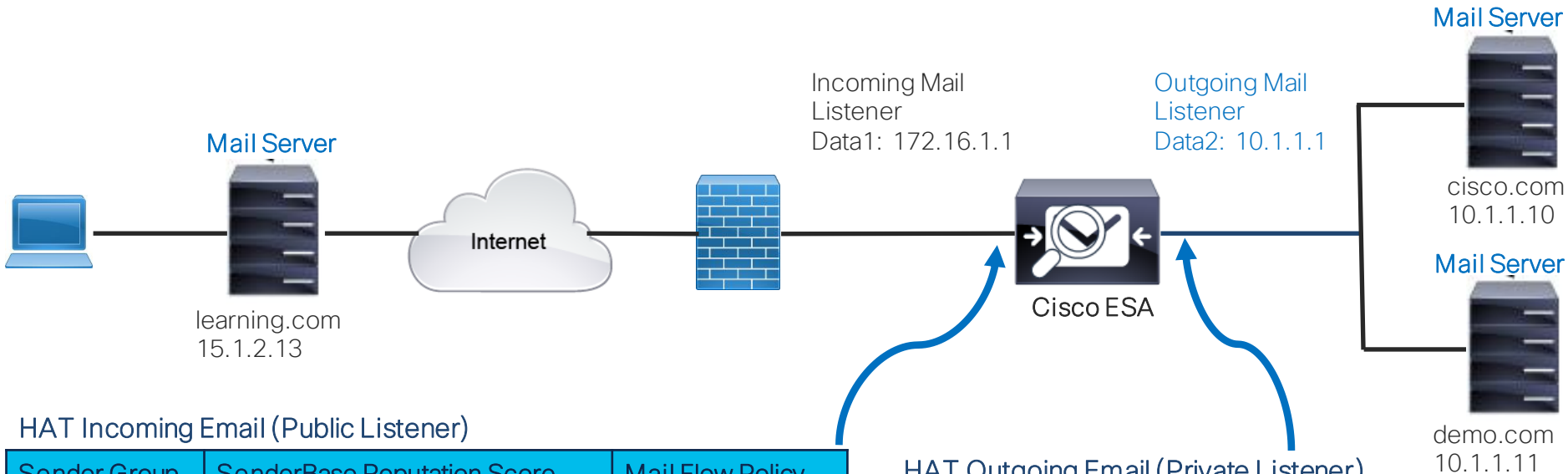


Déploiement Initial

1. Ajouter l'adresse IP de votre serveur SMTP **10.1.1.1** interne dans la table HAT (Relay List)
2. Ajouter votre domaine interne **cisco.com** dans la table RAT



Déploiement une seule interface HAT



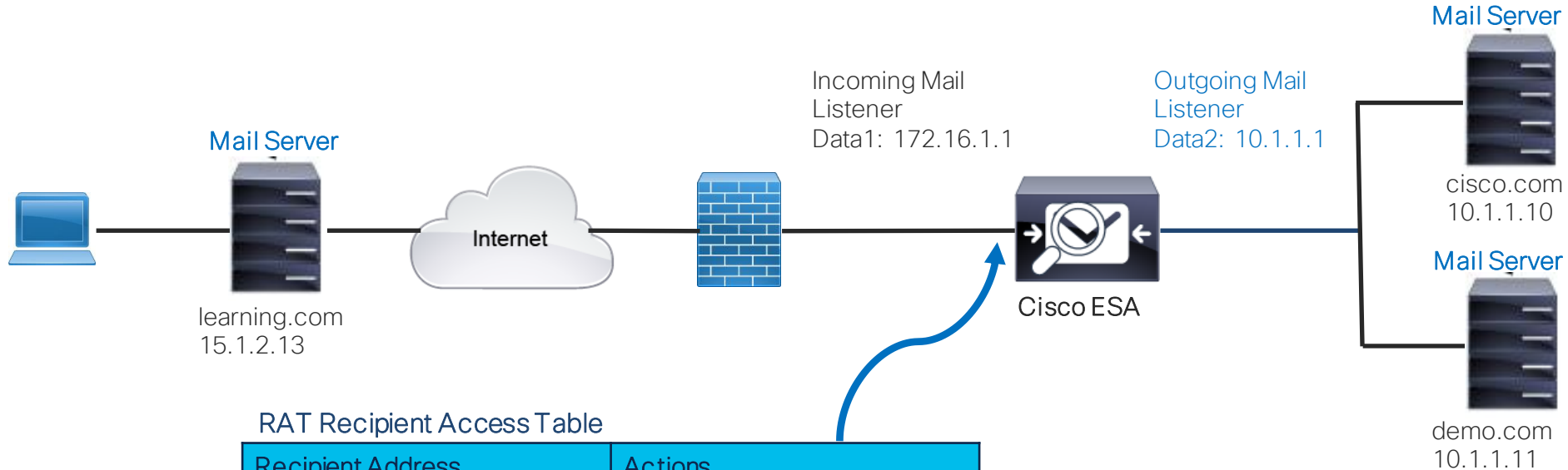
HAT Incoming Email (Public Listener)

Sender Group	SenderBase Reputation Score	Mail Flow Policy
WHITELIST		TRUSTED
BLACKLIST	- 10 to -3	BLOCKED
SUSPECTLIST	- 3 to -1	THROTTLED
UNKOWNLIST	- 1 to 10	ACCEPTED
ALL		ACCEPTED

HAT Outgoing Email (Private Listener)

Sender Group	SenderBase Reputation Score	Mail Flow Policy
RELAYEDLIST		RELAYED
ALL		BLOCKED

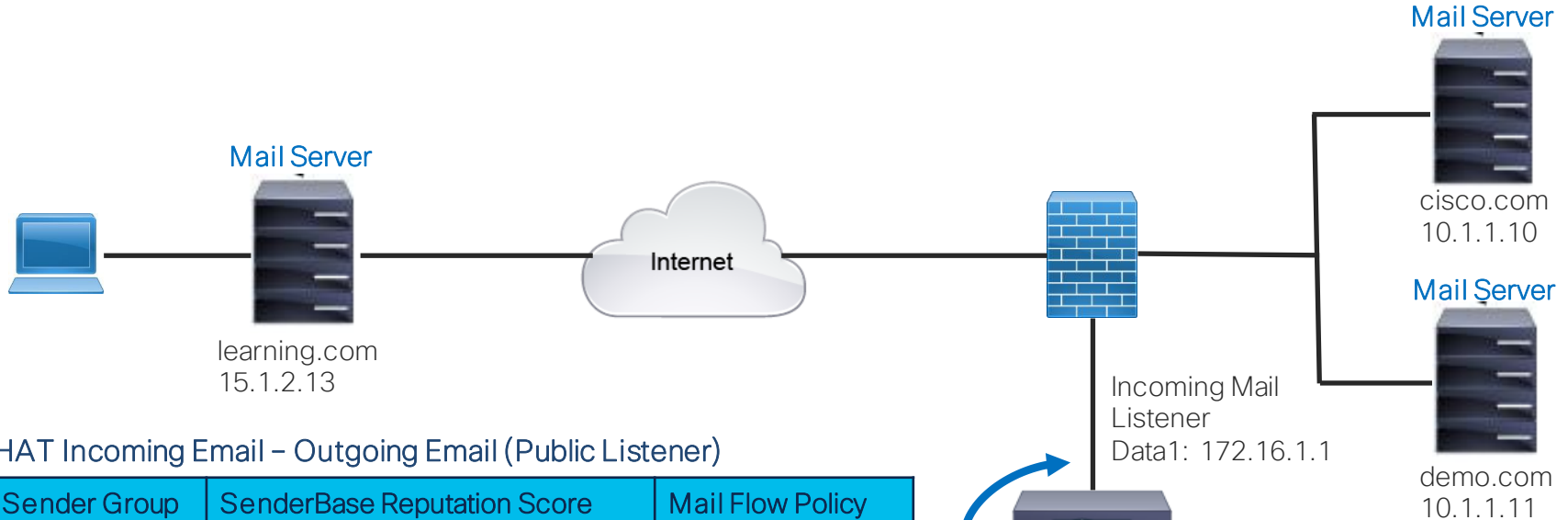
Déploiement une seule interface **RAT**



RAT Recipient Access Table

Recipient Address	Actions
cisco.com	Accept
demo.com	Accept
All other	Reject

Déploiement deux interfaces HAT



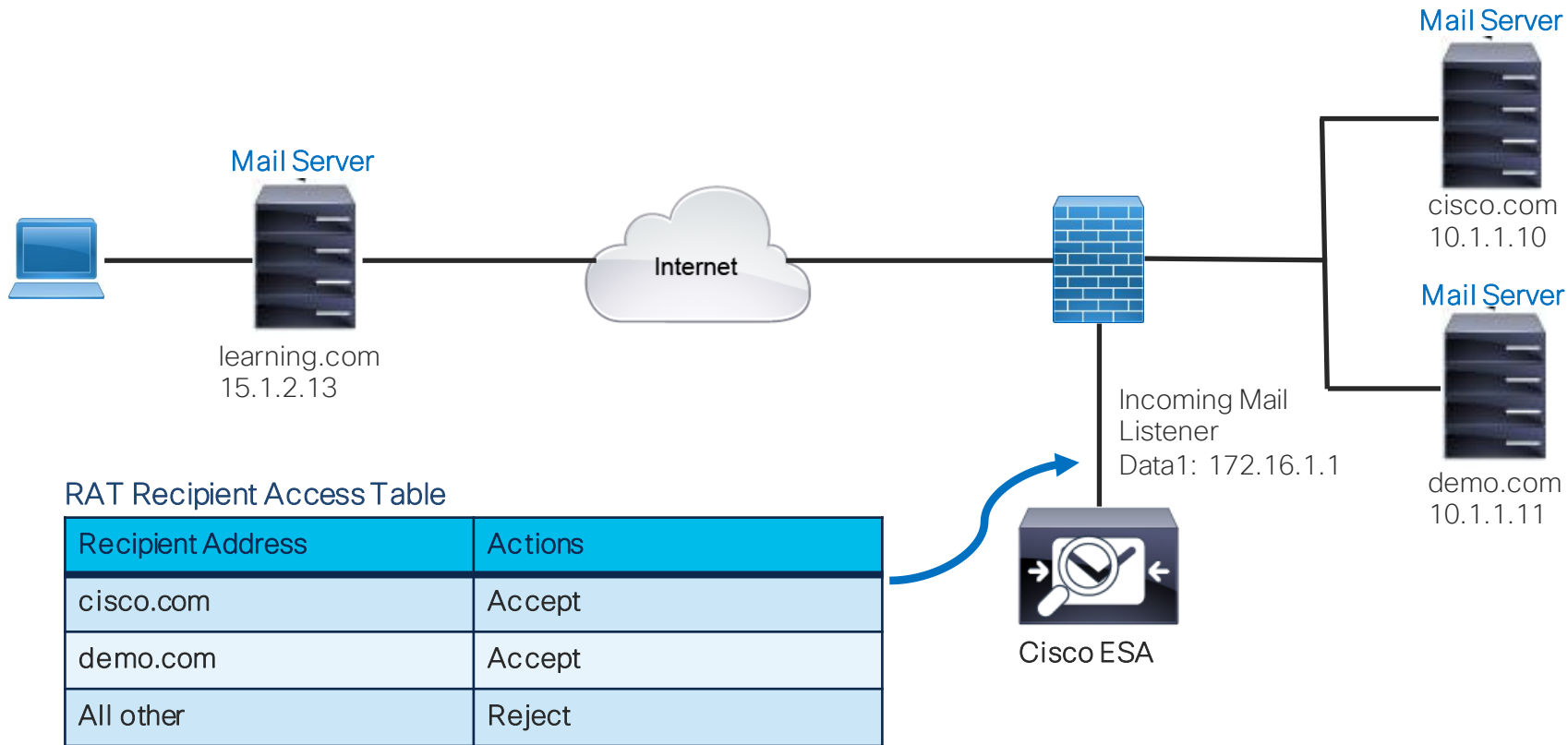
HAT Incoming Email - Outgoing Email (Public Listener)

Sender Group	SenderBase Reputation Score	Mail Flow Policy
RELAYEDLIST		RELAYED
WHITELIST		TRUSTED
BLACKLIST	- 10 to -3	BLOCKED
SUSPECTLIST	- 3 to - 1	THROTTLED
UNKOWNLIST	- 1 to 10	ACCEPTED
ALL		ACCEPTED

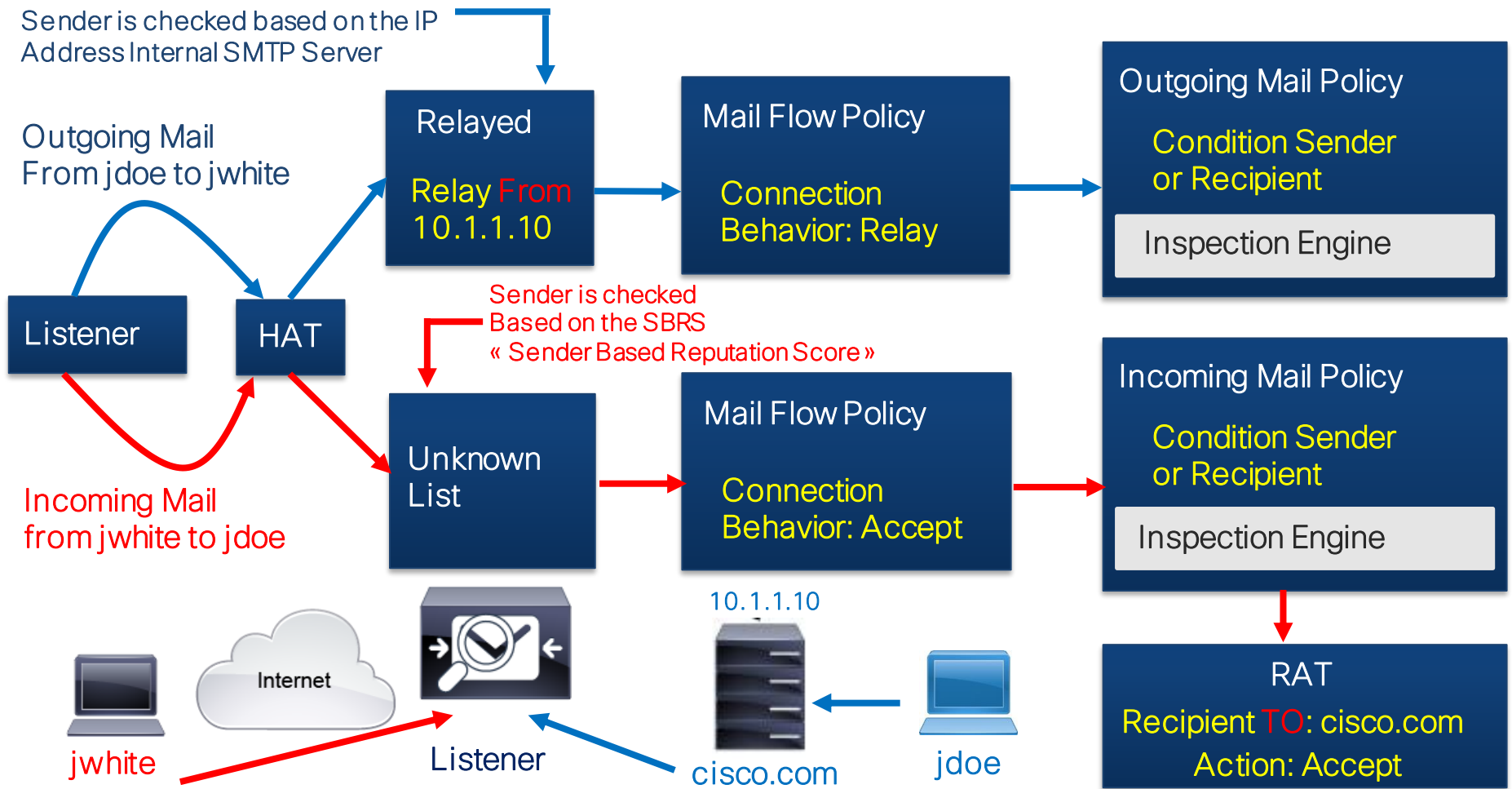


Cisco ESA

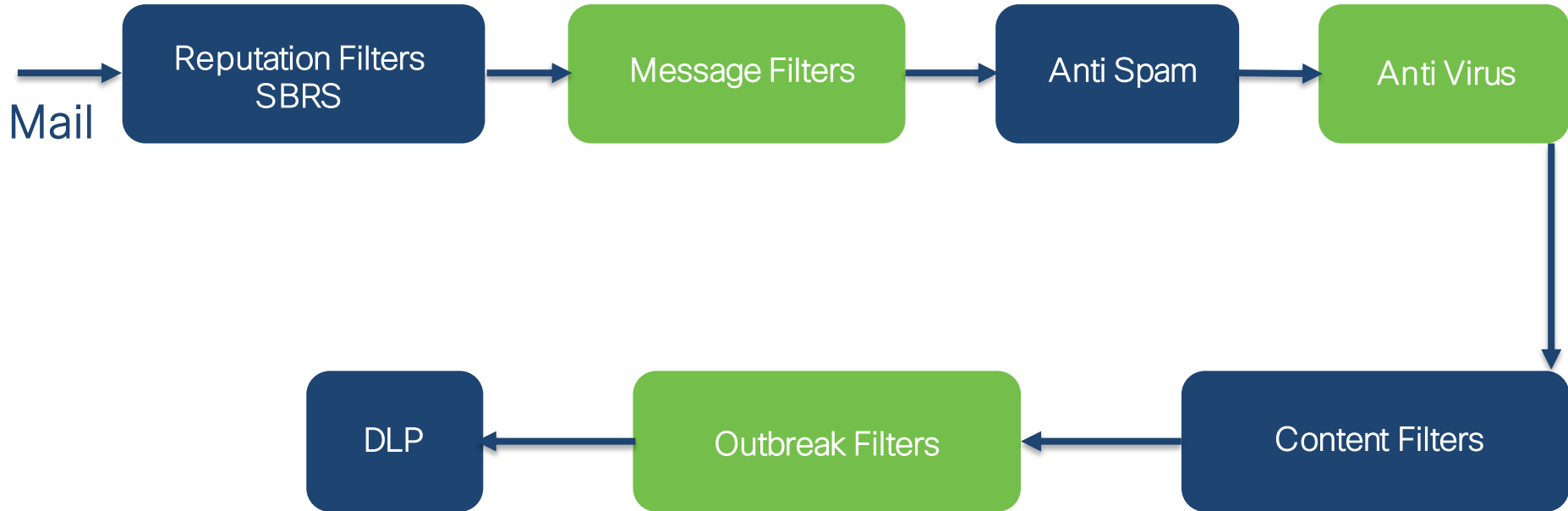
Déploiement deux interfaces RAT



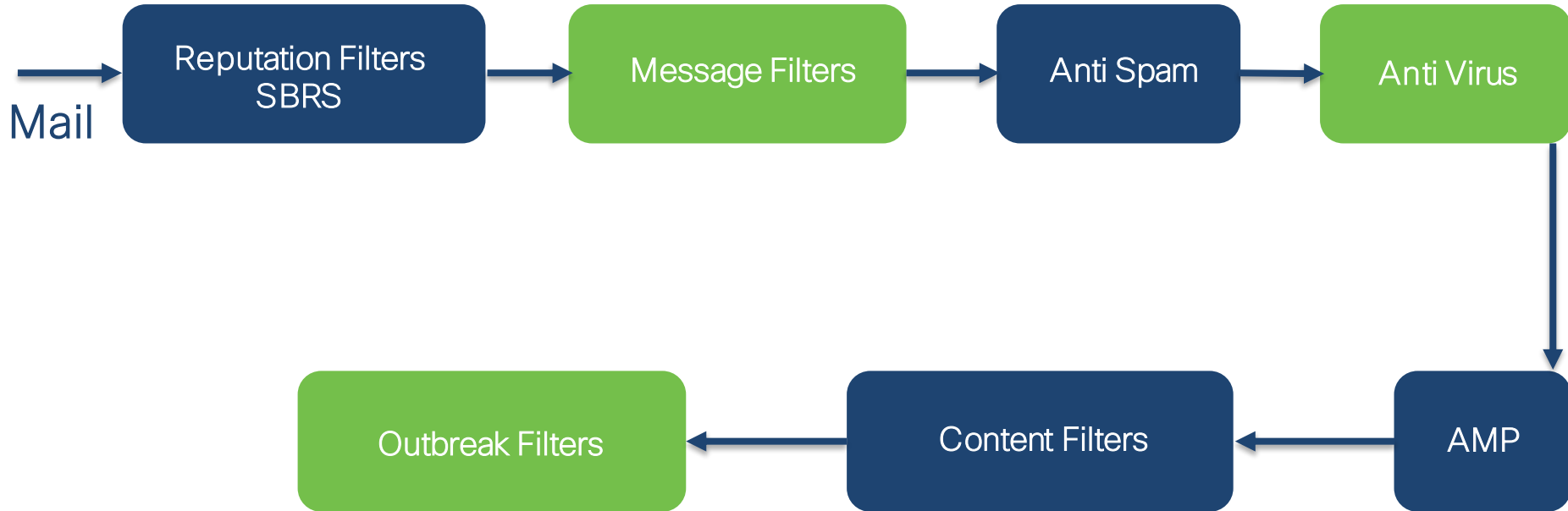
Mail Flow



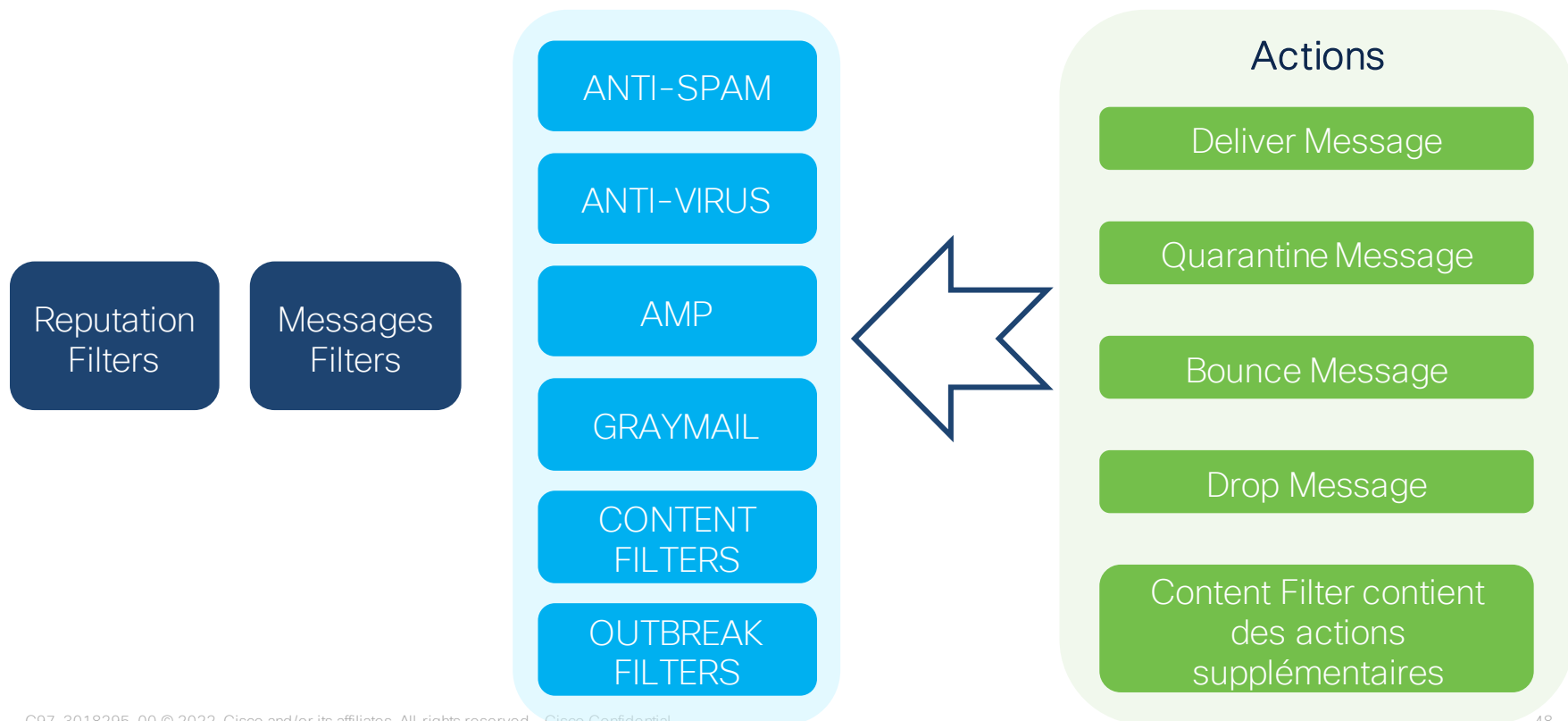
Outgoing Email Flow (Inspection Engine)



Incoming Email Flow (Inspection Engine)



Actions sur les messages



Polling Question 3

Dans quel listener on définit la table RAT?
(Recipient Access Table)

- 1) Private Listener
- 2) Public Listener
- 3) Les deux listeners Private et Public

Avez-vous encore des questions ?

Nos experts vous répondent

Si vous avez posé une question sur le panneau de Q&R (Q&A en anglais) ou que vous revenez sur la communauté dans les jours qui suivent notre webinaire, nos experts peuvent encore vous aider !

Participez dans le forum de Ask Me Anything (AMA) avant le 25 novembre 2022

<https://bit.ly/AMA-nov22>



Nos réseaux sociaux



LinkedIn

[Cisco Community](#)

Twitter

[@cisco_support](#)

YouTube

[CiscoSupportChannel](#)

Facebook

[CiscoSupportCommunity](#)





Faites valoir votre opinion
en répondant à notre enquête !

Cliquez sur le lien

<https://bit.ly/WEBenq-nov22>



The bridge to possible