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

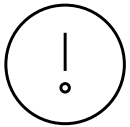
le mardi 22 novembre 2022

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

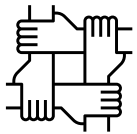
Acceptez les solutions qui sont correctes et complimentez ceux qui vous ont aidé ! Aidez autres utilisateurs à trouver les réponses correctes dans la fenêtre de recherche.

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

Community Spotlight awards

Redouane Meddane

Présentateur

Redouane Meddane est Instructeur Cisco CCSI №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

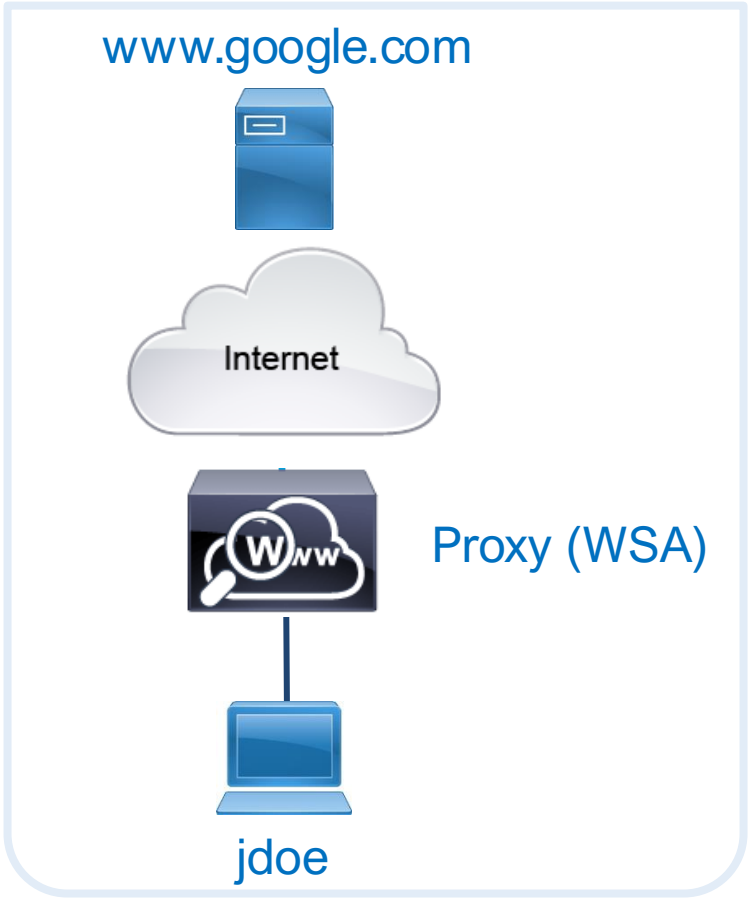
Bandwidth Limits

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 »

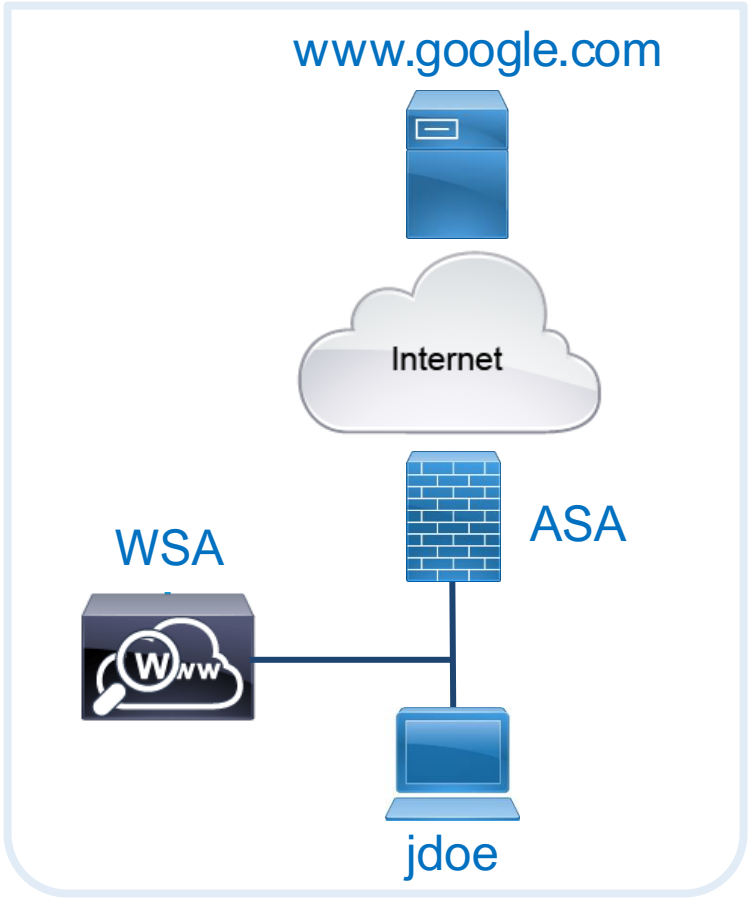
Explicit Forward Mode

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
- Authentification
- Pas authentification

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

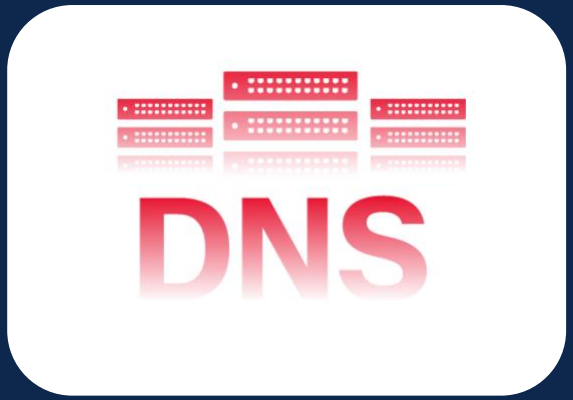
En mode Explicit Forward, quelle est l'entité qui fait la résolution DNS ?

1) Client
2) WSA
3) Firewall

Cisco Umbrella

L’importance du DNS

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

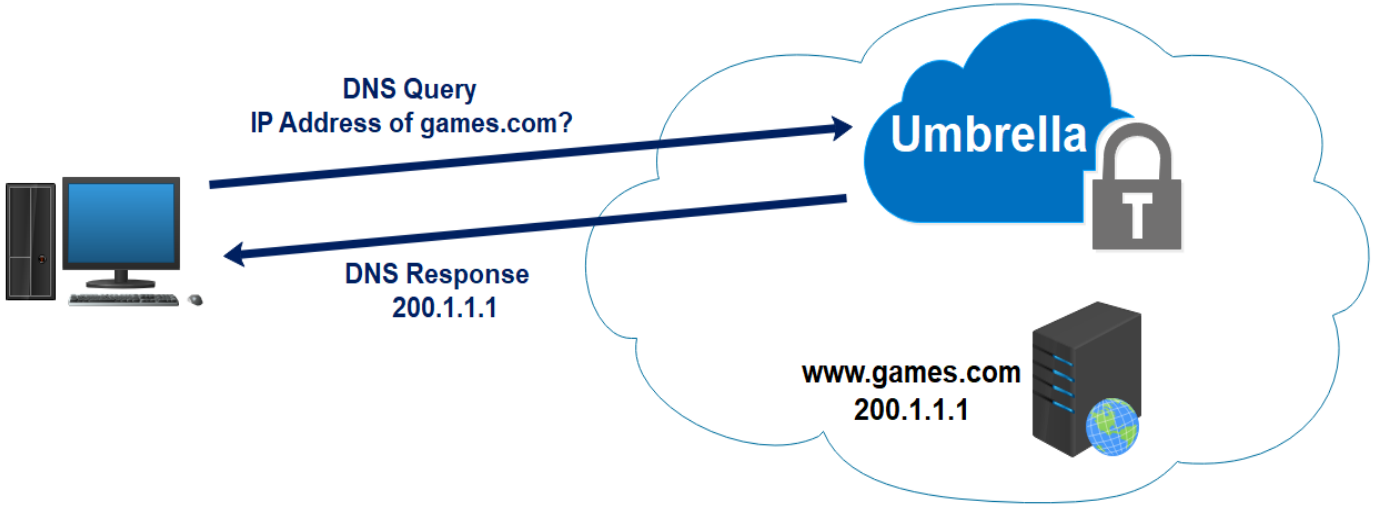


91.3% des attaques malware utilisent DNS

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

Umbrella comme service DNS

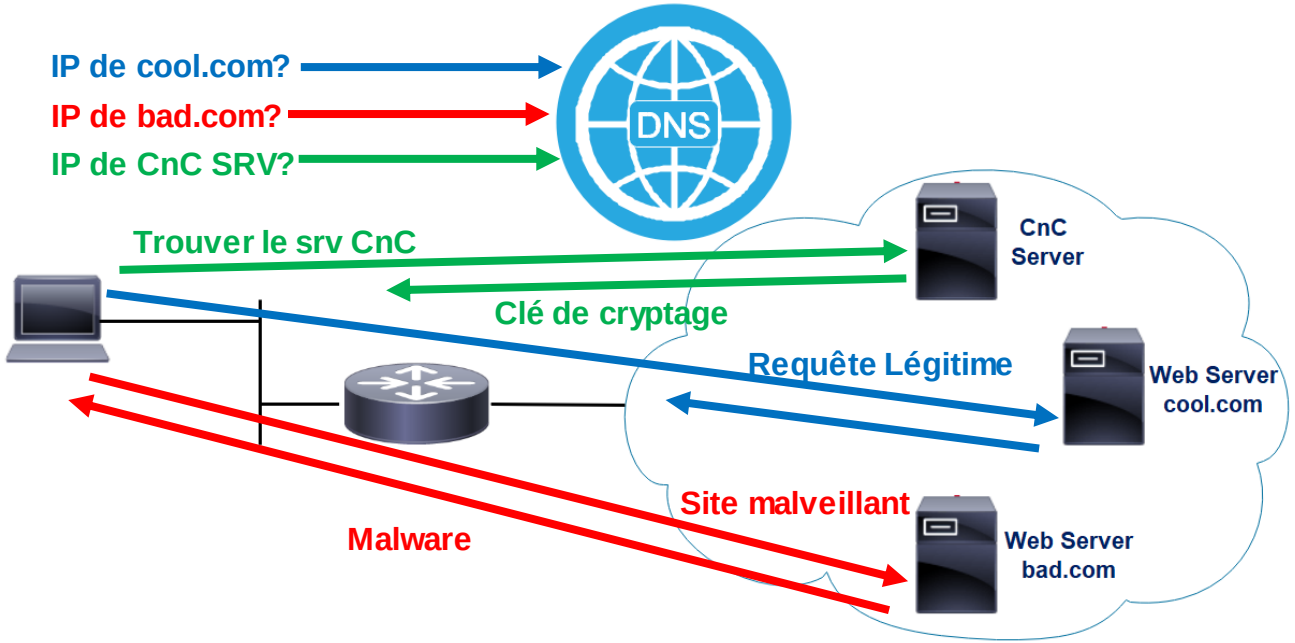
Tout commence par le DNS.
Umbrella est un service DNS.
Le DNS précède l'exécution du fichier et la connexion IP.



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 ur host infecté?



Umbrella n’est pas qu’un service DNS

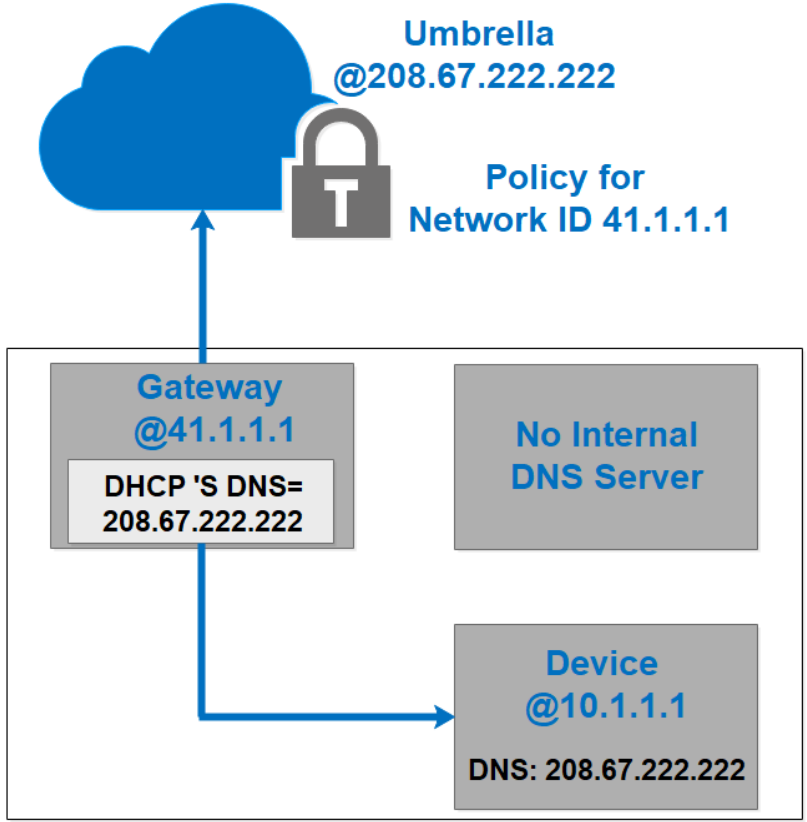
- Threat Prevention
- Protection On & Off Network
- Block par Domains, IPs & URLs
- Proxy et inspection des fichiers (Intelligent proxy, SSL Decryption)

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.

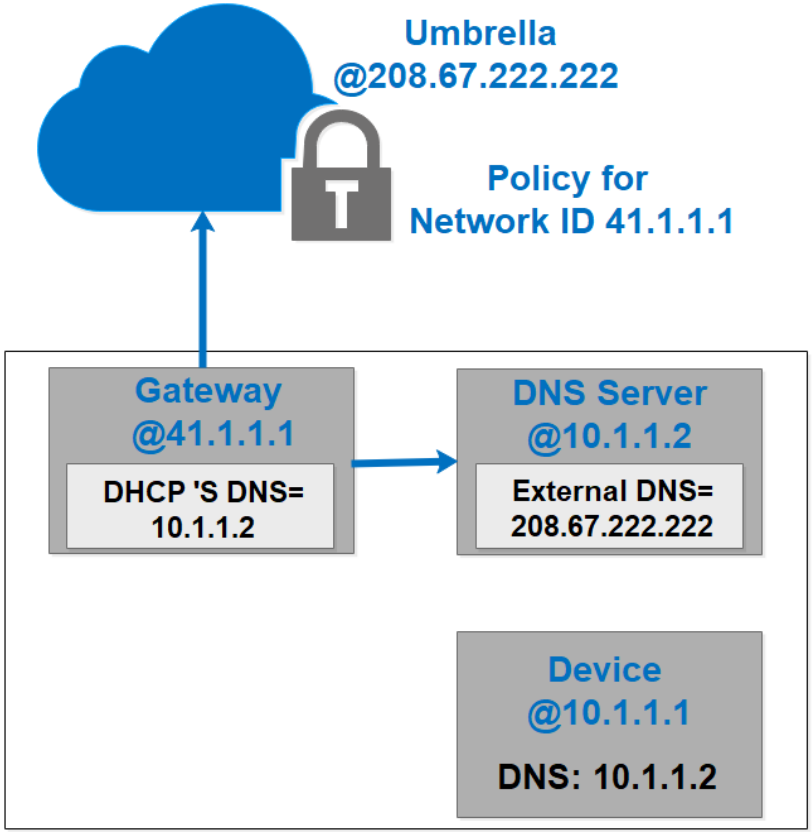


Déploiement avec serveur DNS interne

- 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.

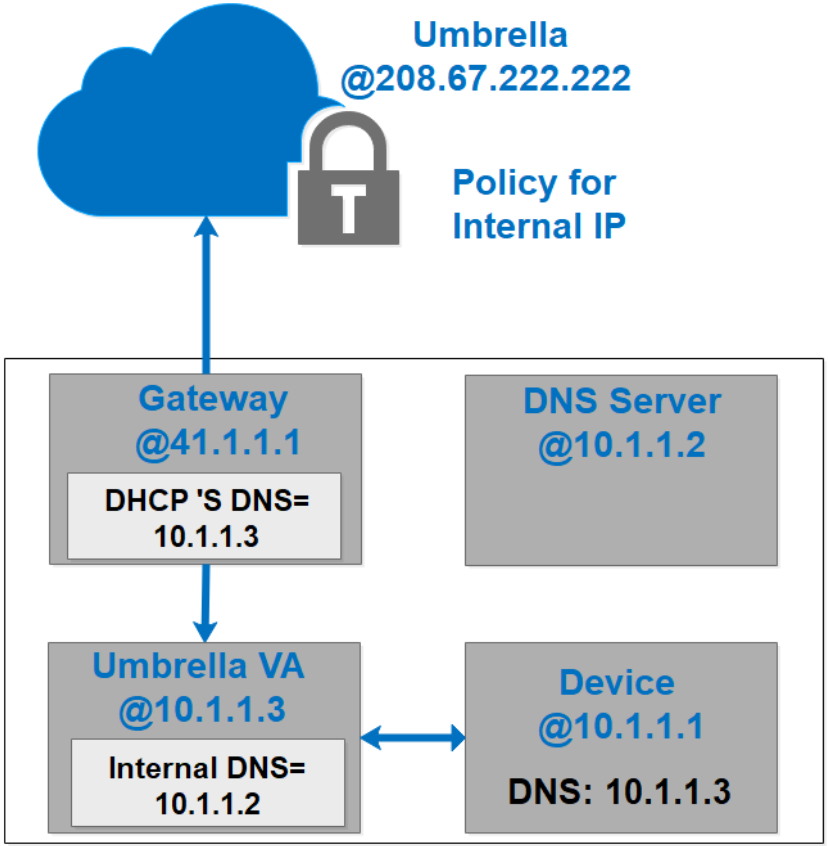


Déploiement avec une appliance virtuelle Umbrella VA

- 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.

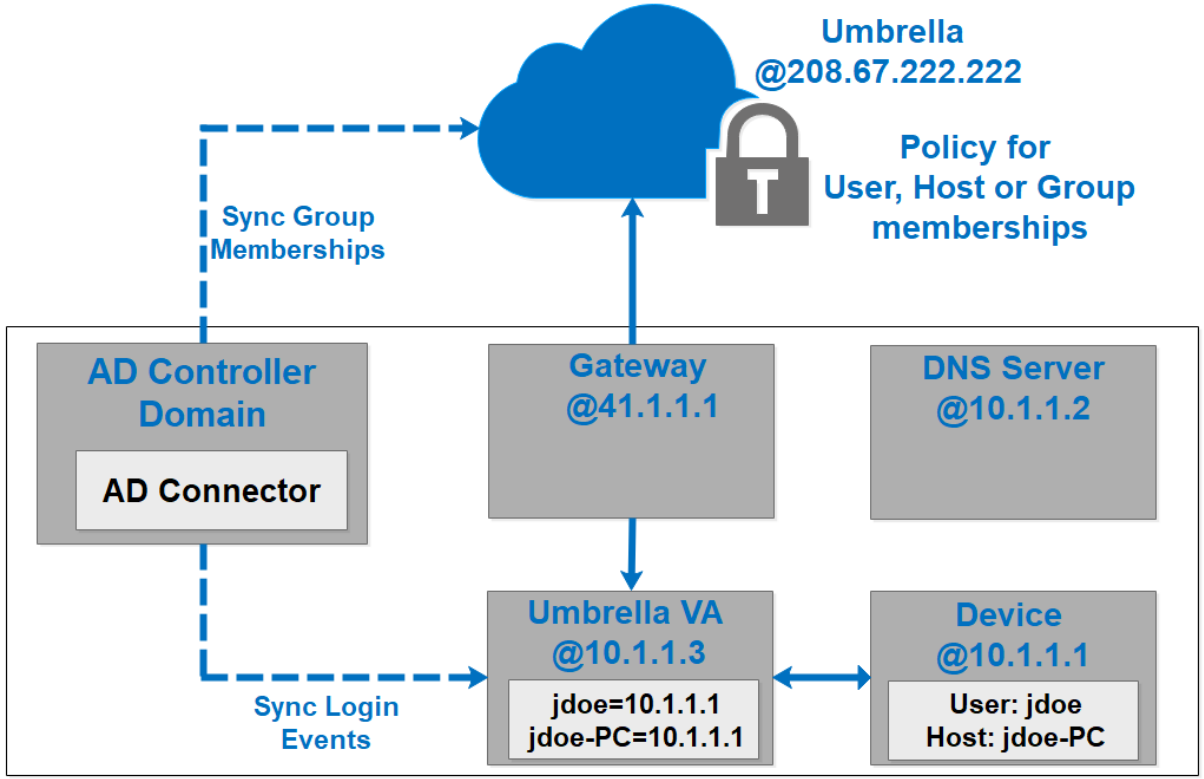


Déploiement avec une VA Umbrella et Active Directory

- Synchronisation des groupes AD/Users AD avec Umbrella

Considérations

Des policies basées sur les groupes AD/Users AD.



Déploiement avec un client Umbrella

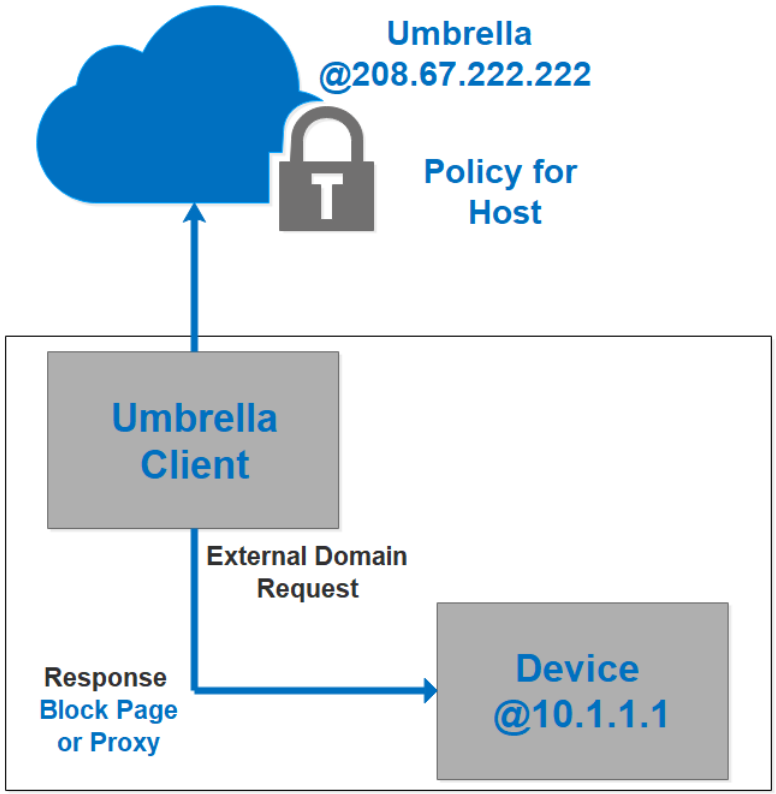
- Protection OFF-Network (Télétravail) et On-Network.
- Un client Umbrella installé dans le PC, les requêtes DNS sont redirigées vers Umbrella.

Considérations

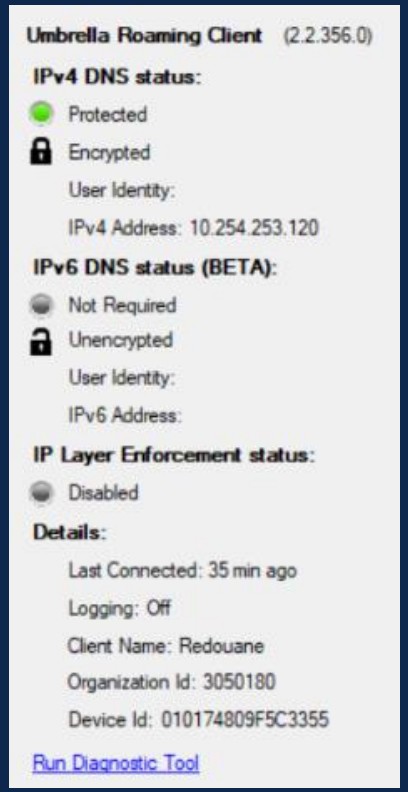
Des policies basées sur le nom des machines.

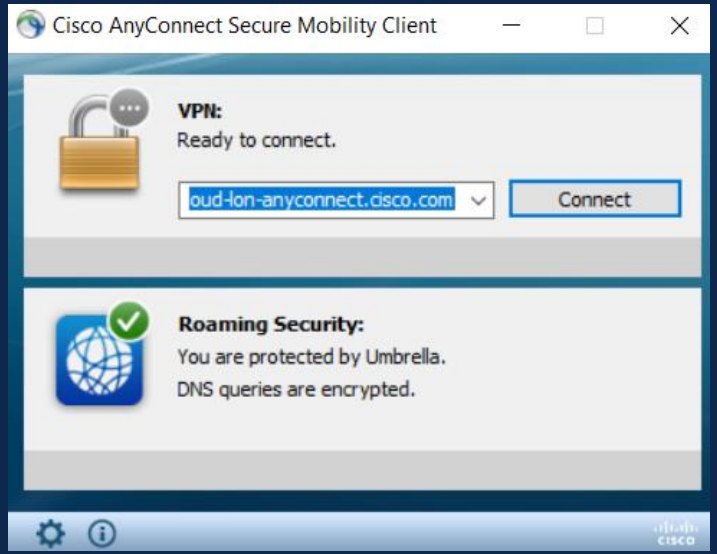
Deux clients:

Umbrella Roaming Client
Roaming Security AnyConnect Module.

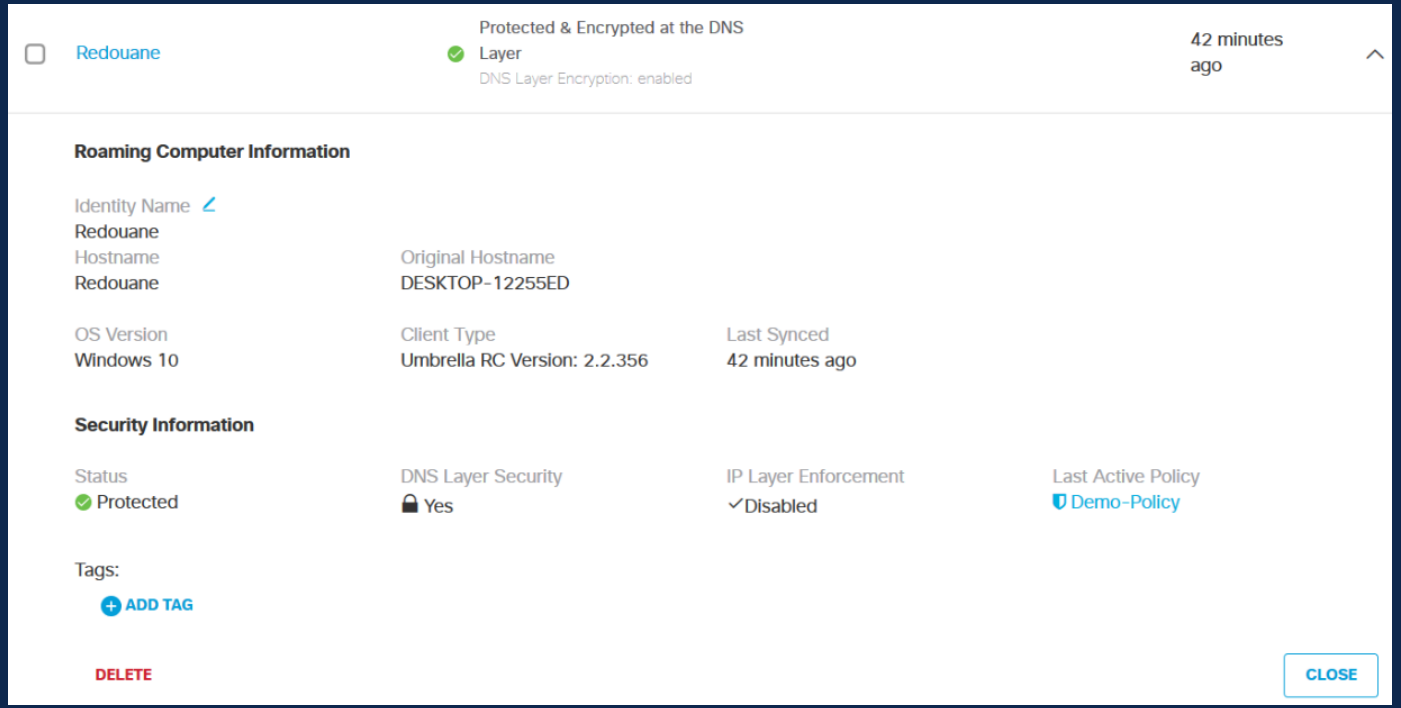


Client Umbrella

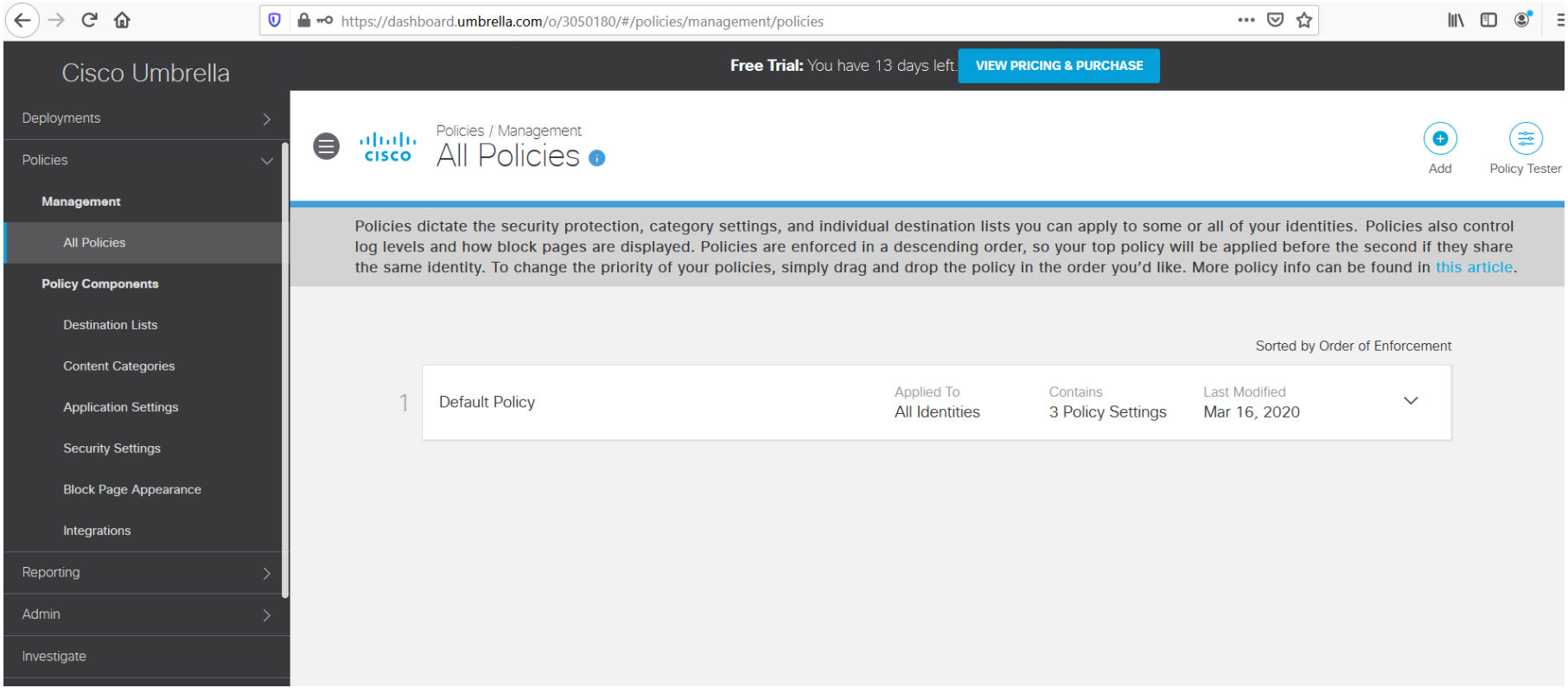




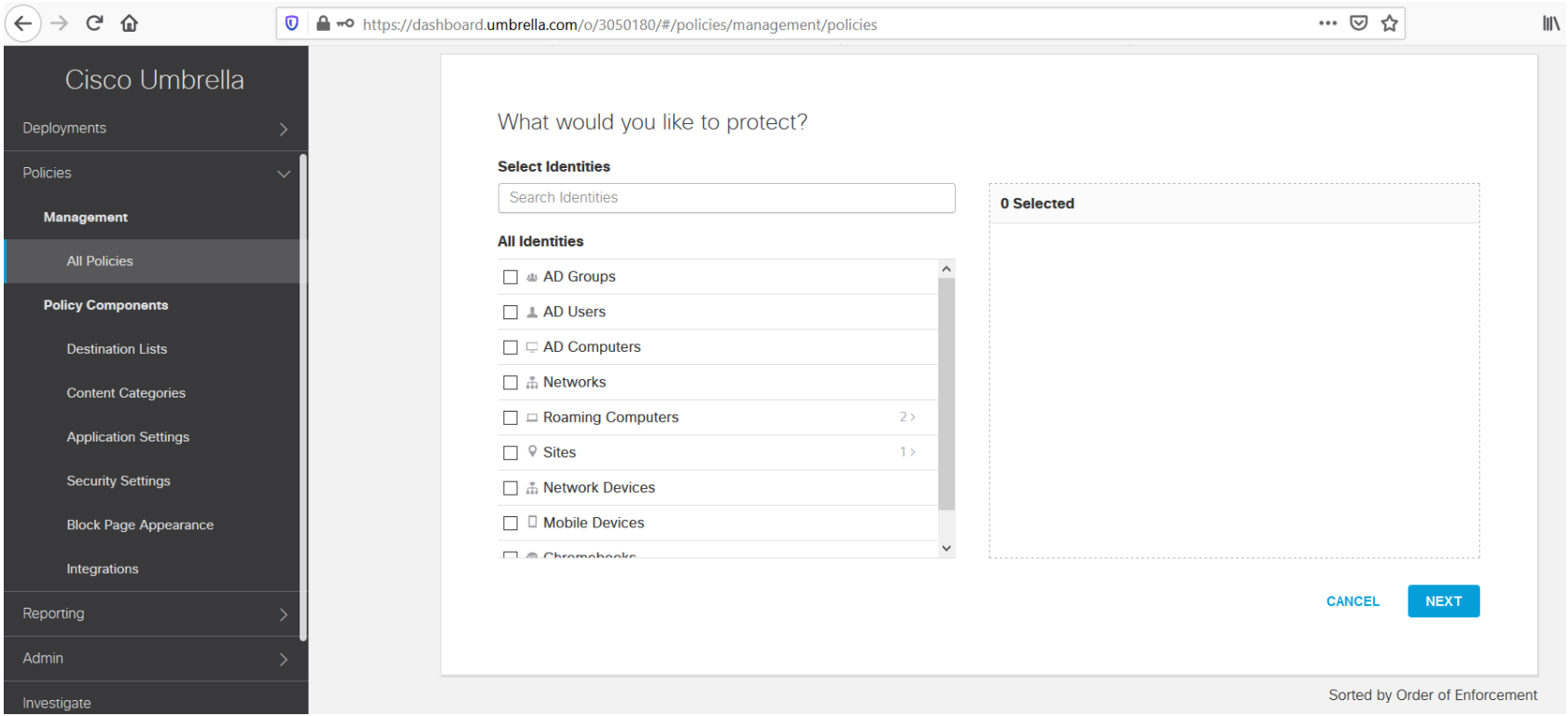
A la découverte de l'interface graphique



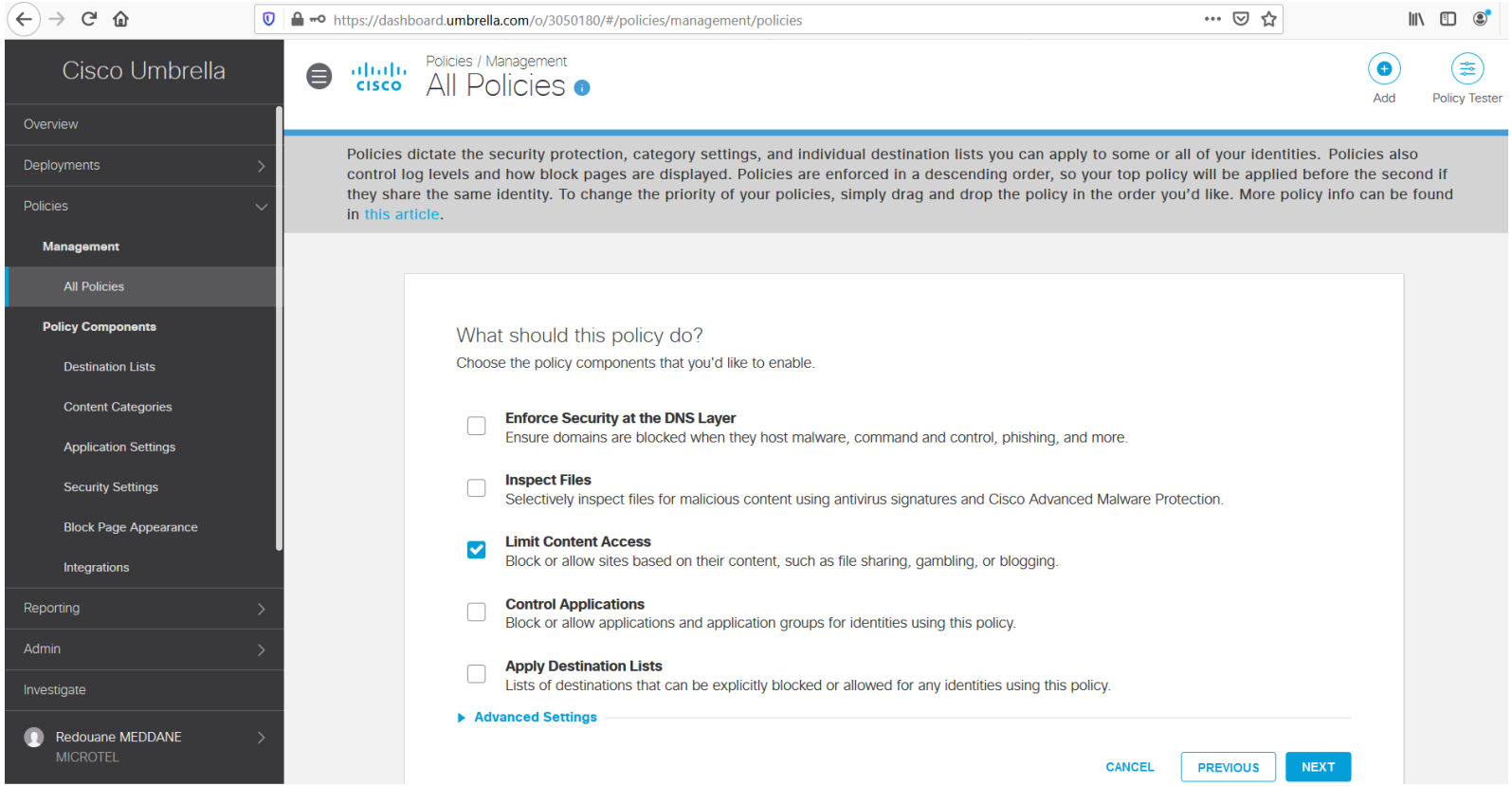
Policies



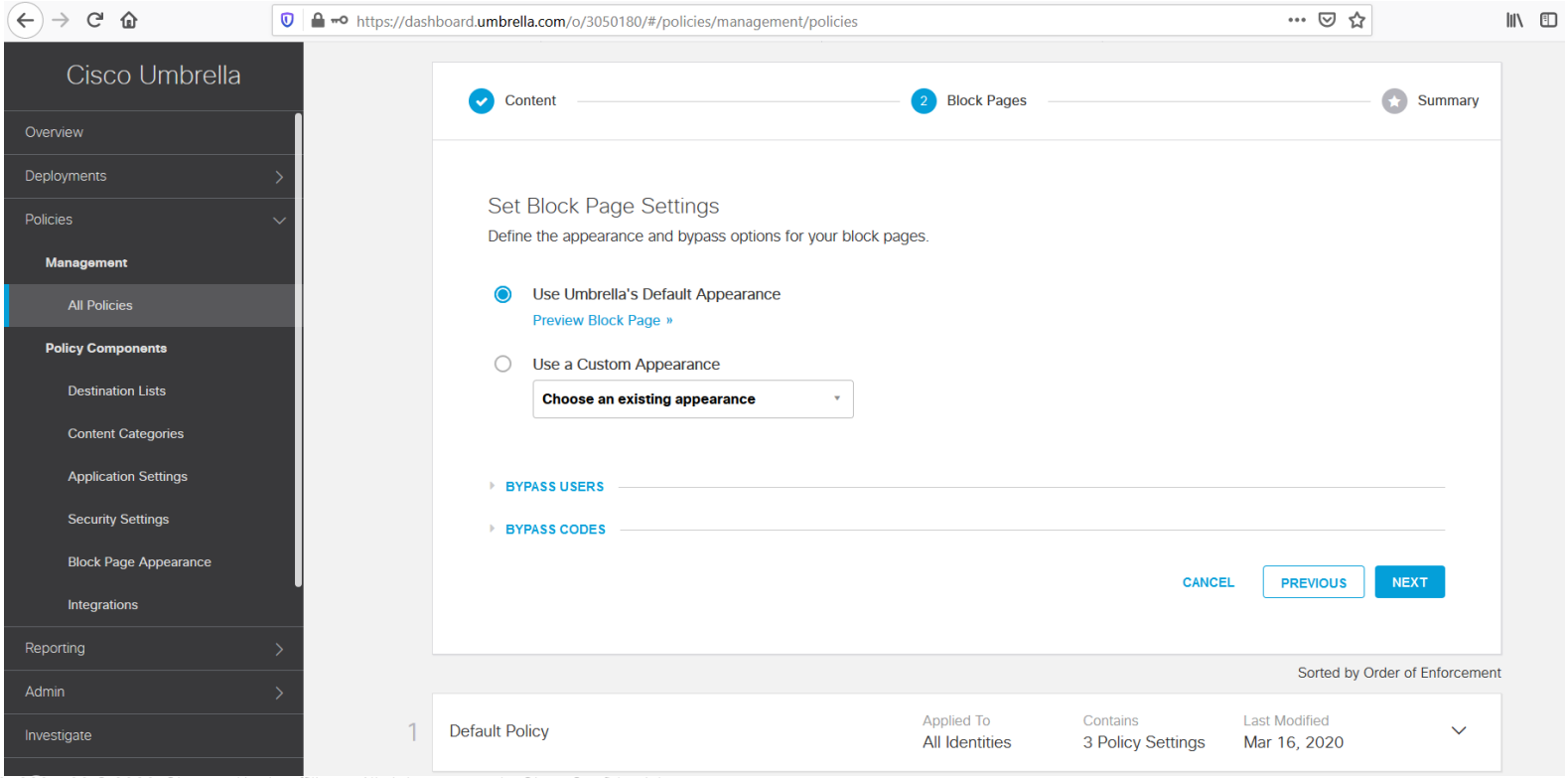
Création d'une policy - Conditions



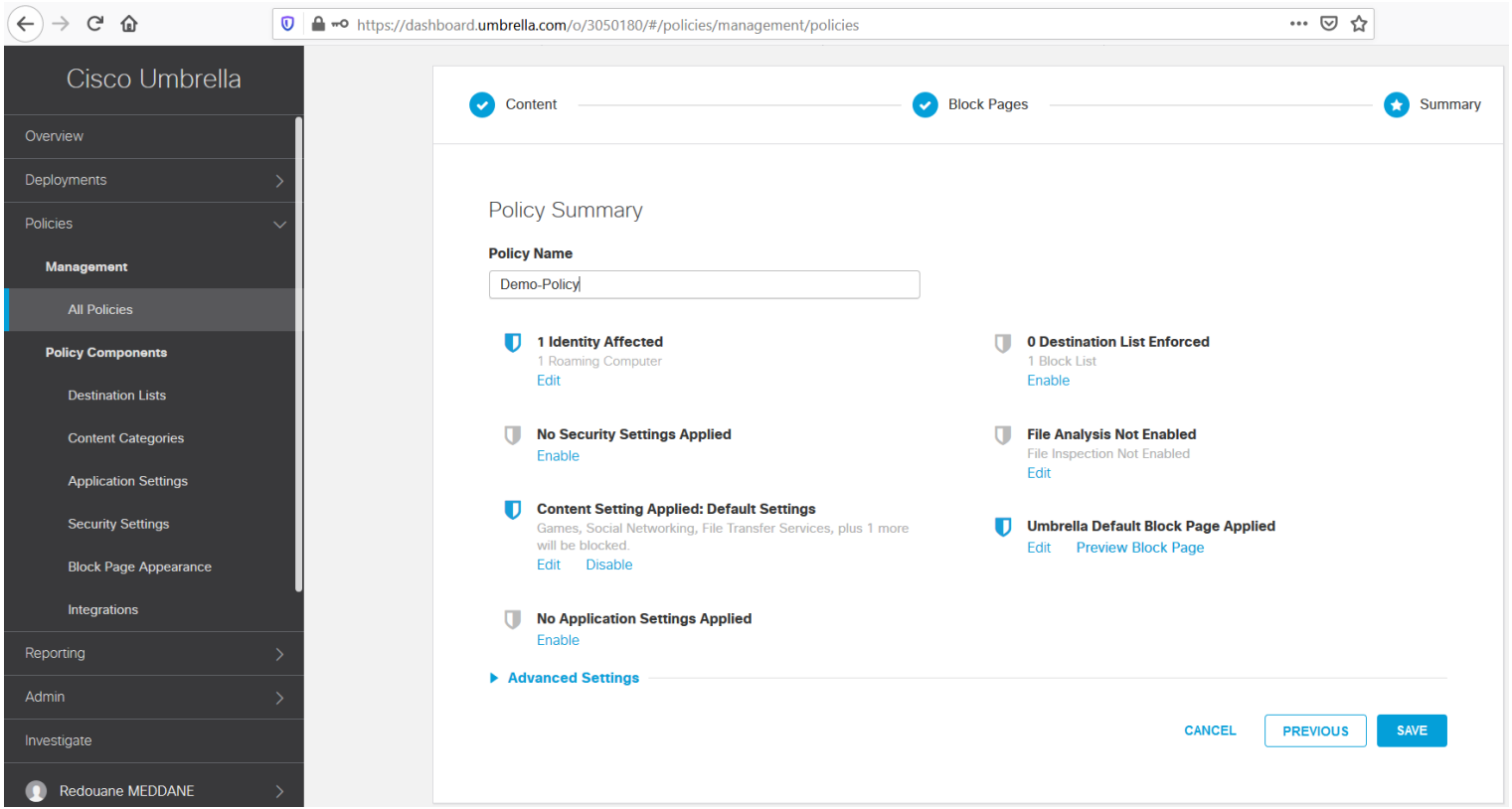
Création d'une policy - Filtres



Création d'une policy – Block Page

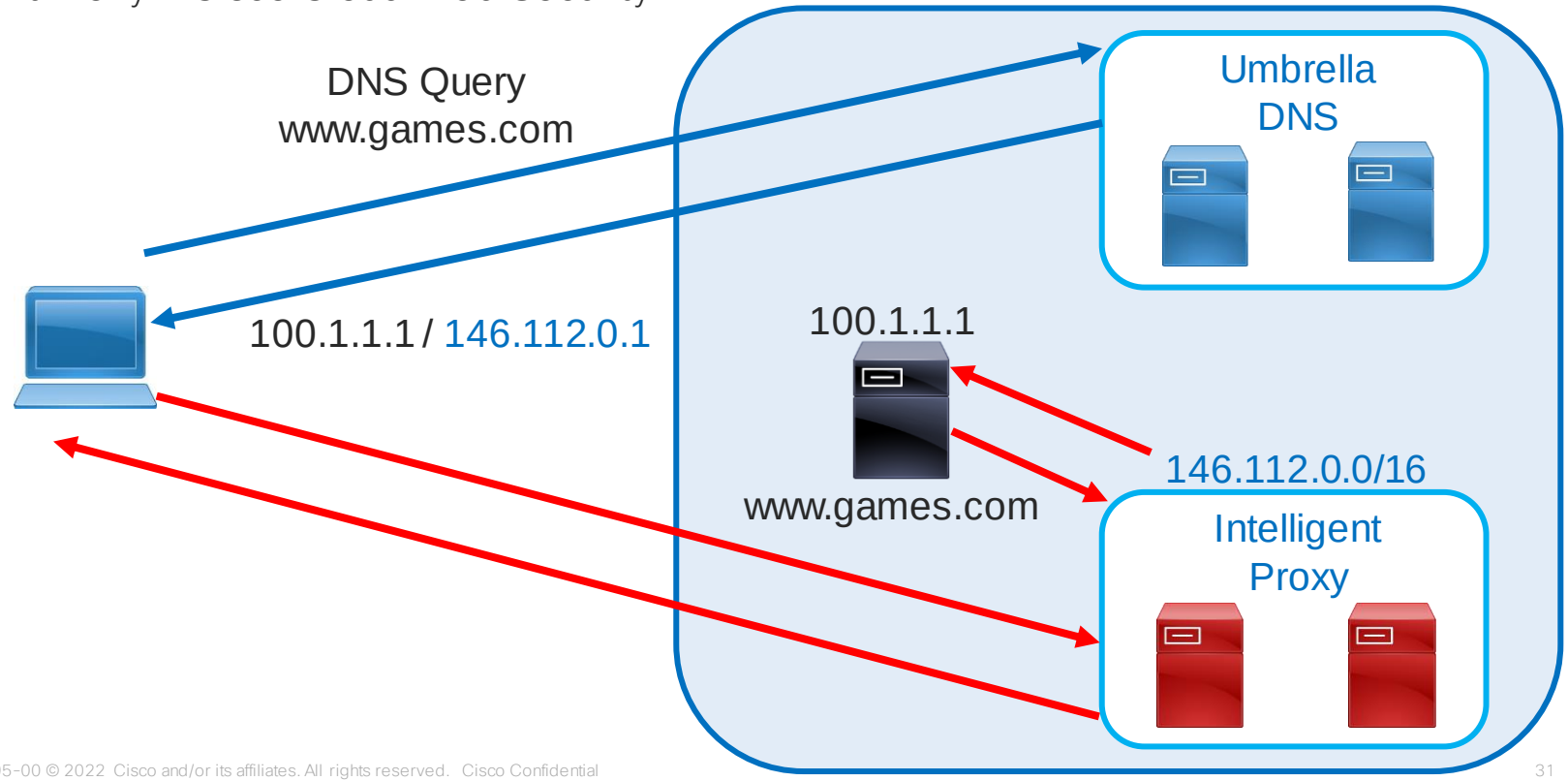


Création d'une policy – Intelligent Proxy

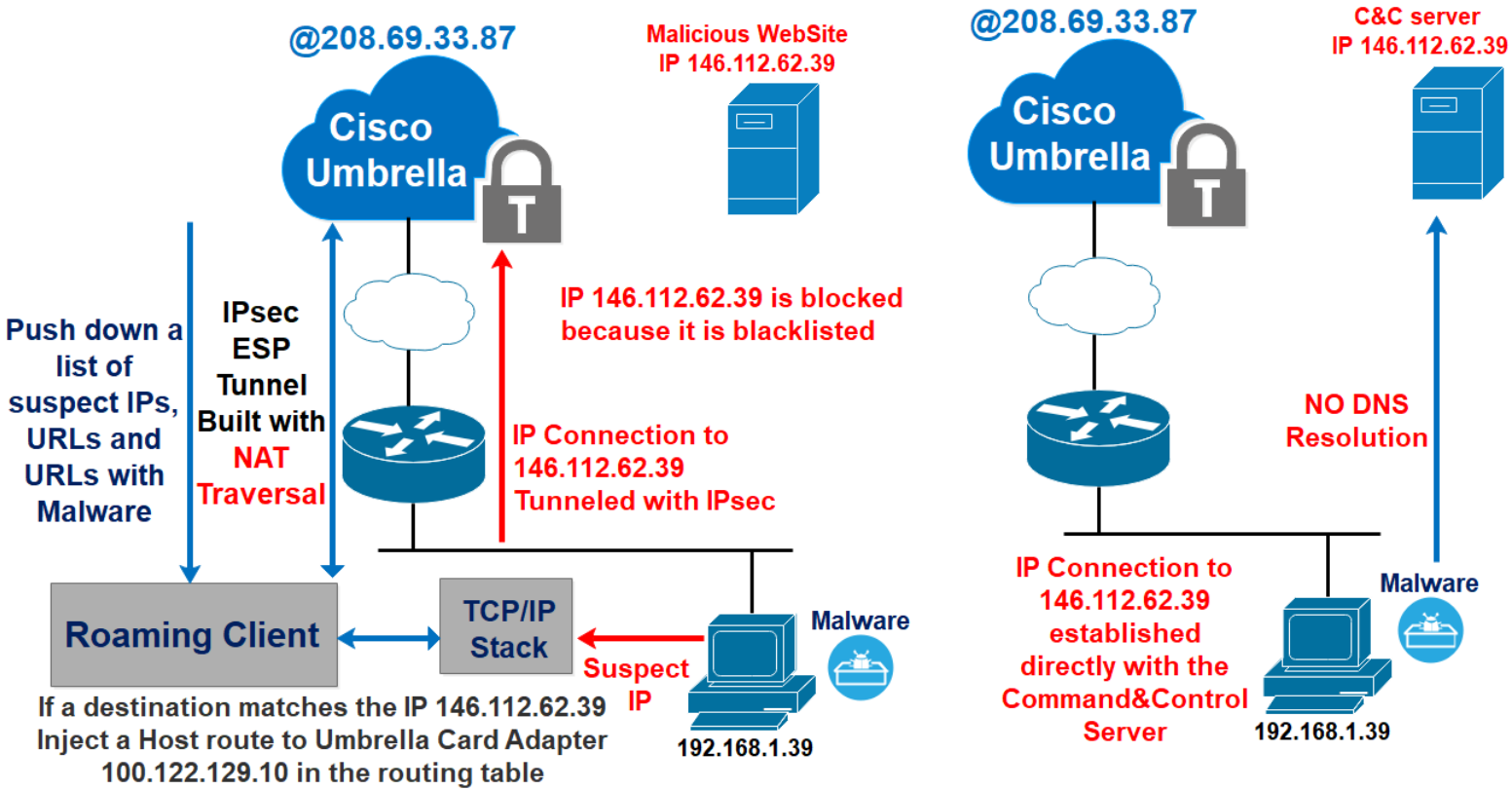


Intelligent Proxy

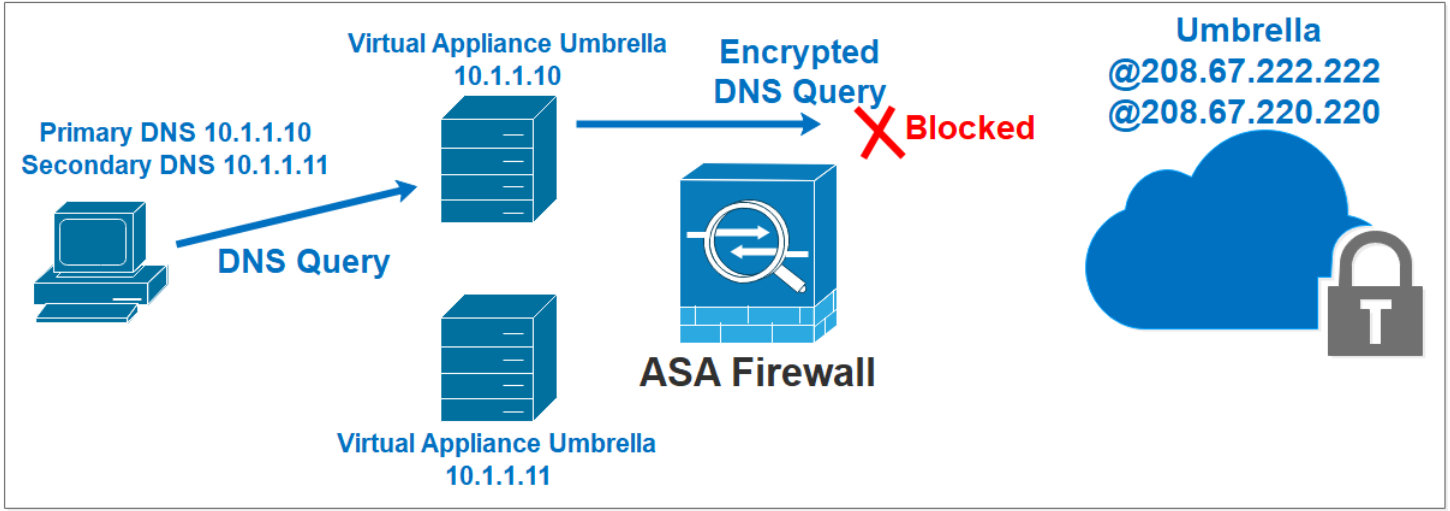
Intelligent Proxy = Cisco Cloud Web Security



IP Layer Enforcement



Use case



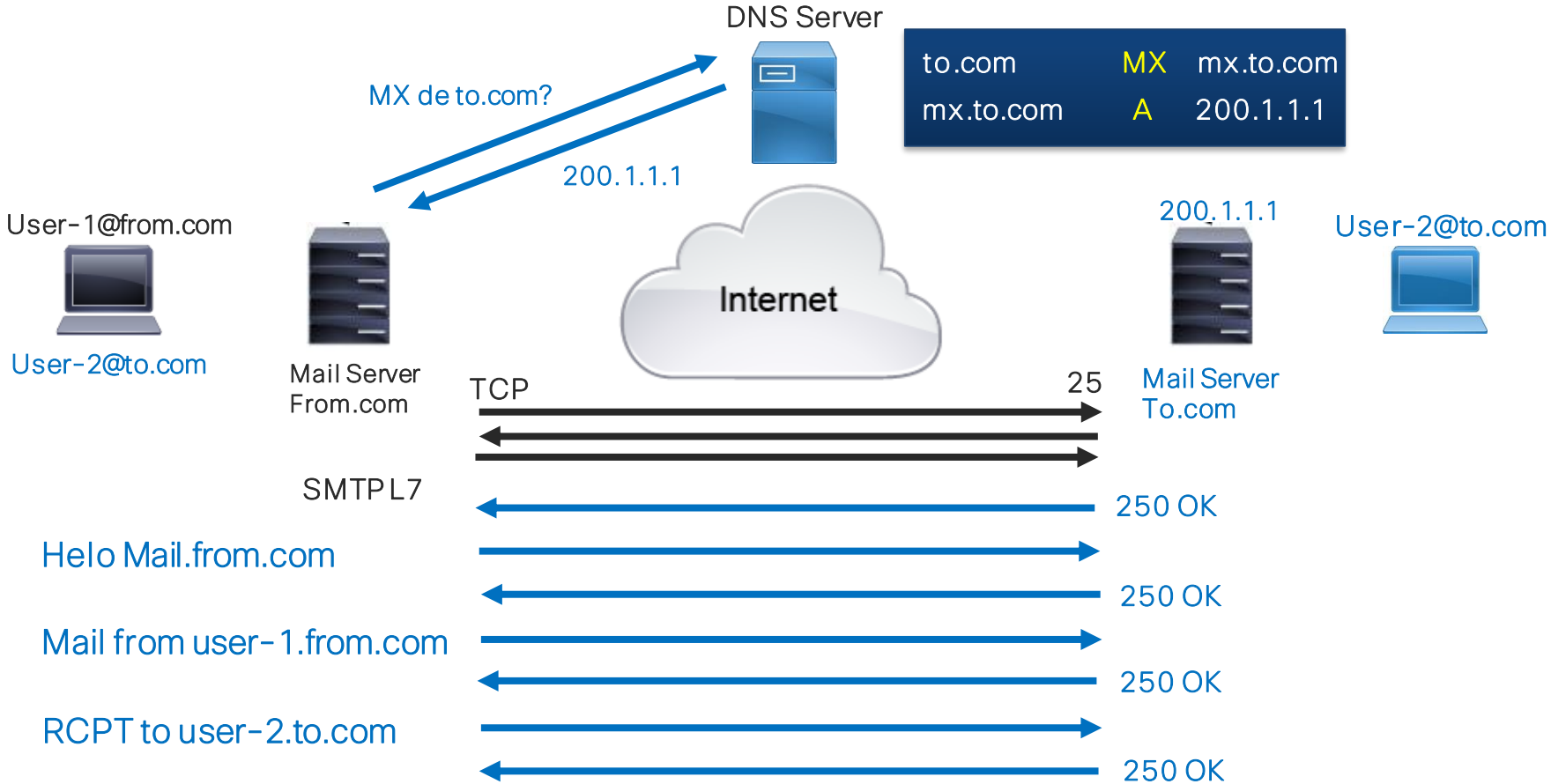
Polling Question 2

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

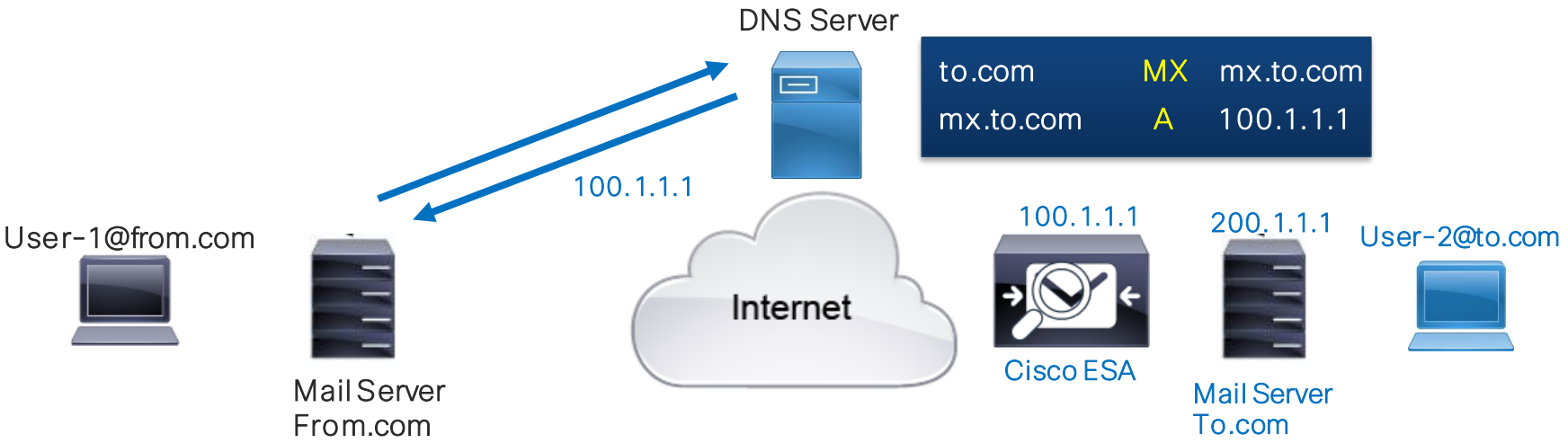
1) Bypasser les firewalls Edge
2) Bypasser la couche Security DNS
3) Bypasser le proxy Umbrella (Intelligent Proxy)

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

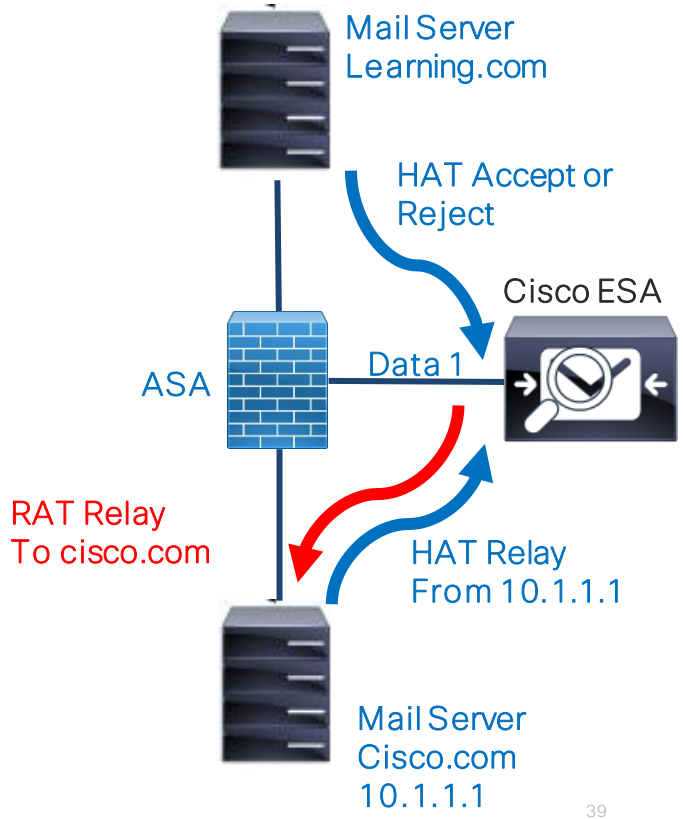
RAT: Recipient Access Table

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.

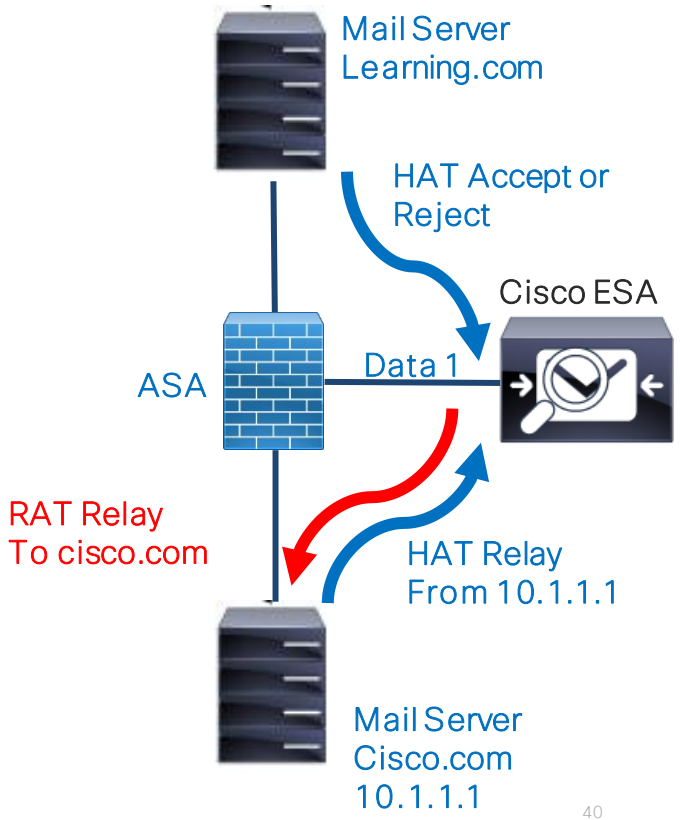
- **Private listener (Outgoing mail):** Nous avons besoin du HAT seulement pour relayer les mails sortants émanant de notre serveur SMTP interne.



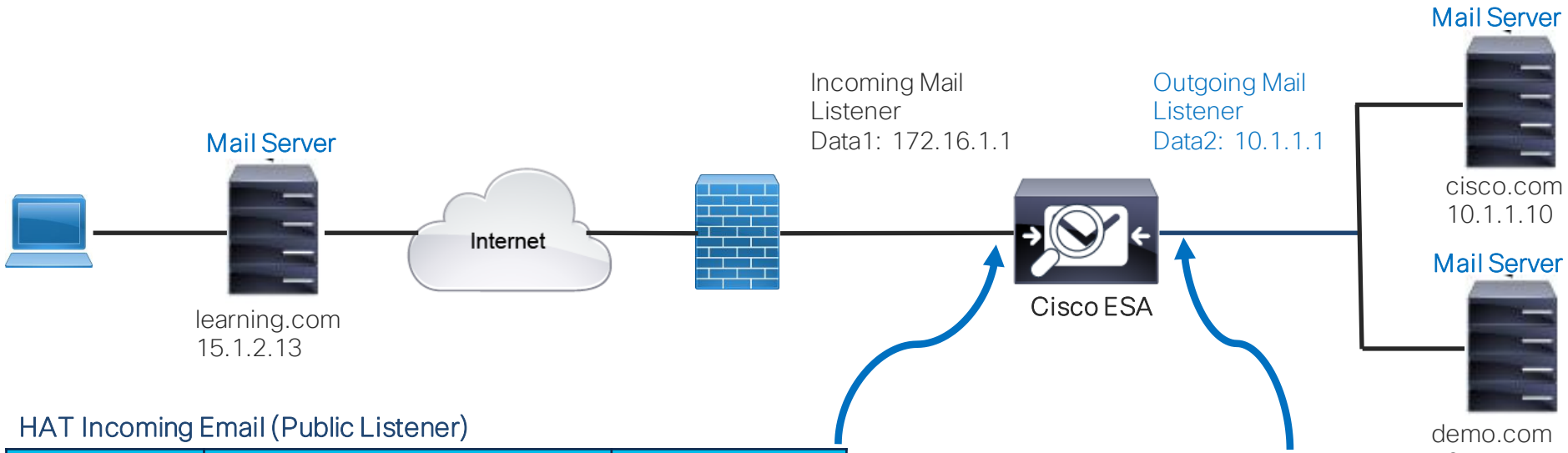
Déploiement Initial

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



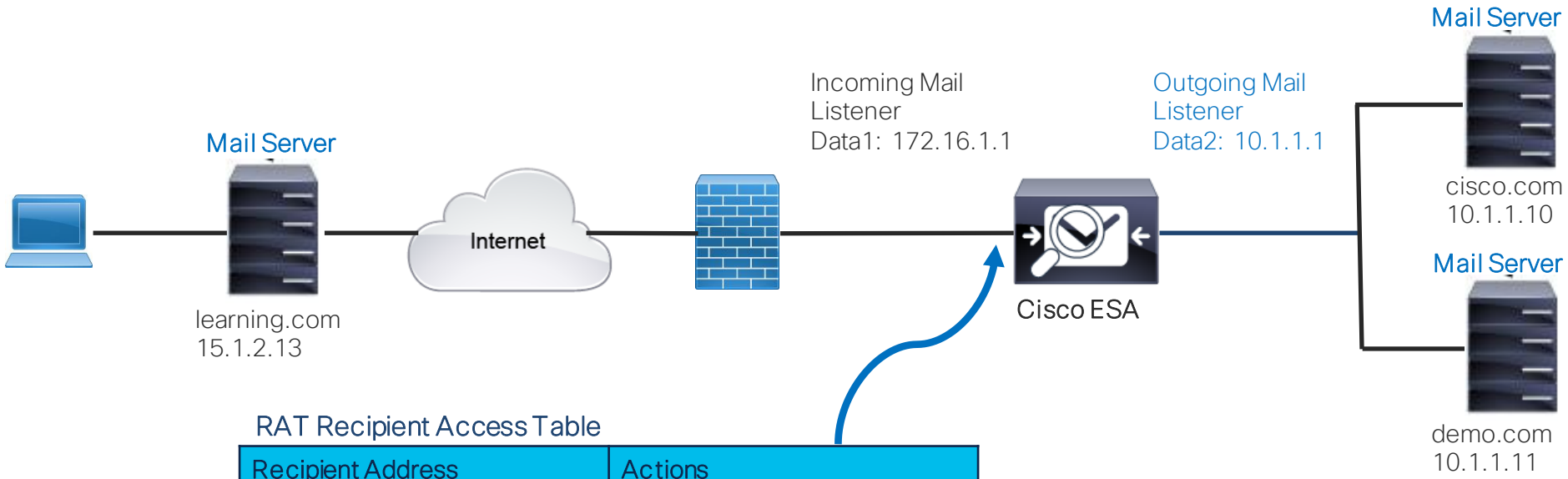
HAT Incoming Email (Public Listener)

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

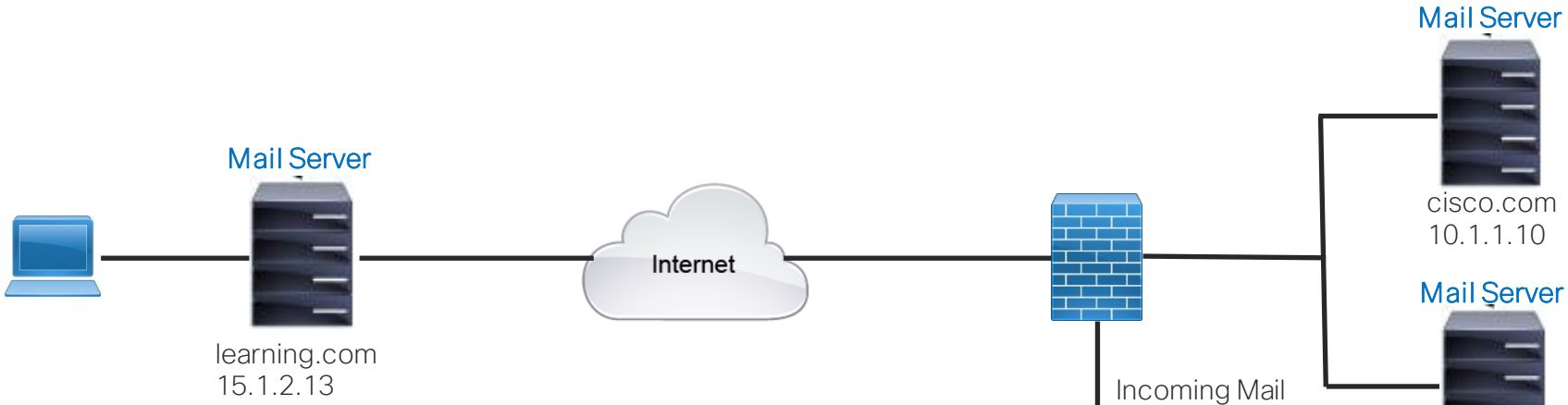
Déploiement une seule interface RAT



RAT Recipient Access Table

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

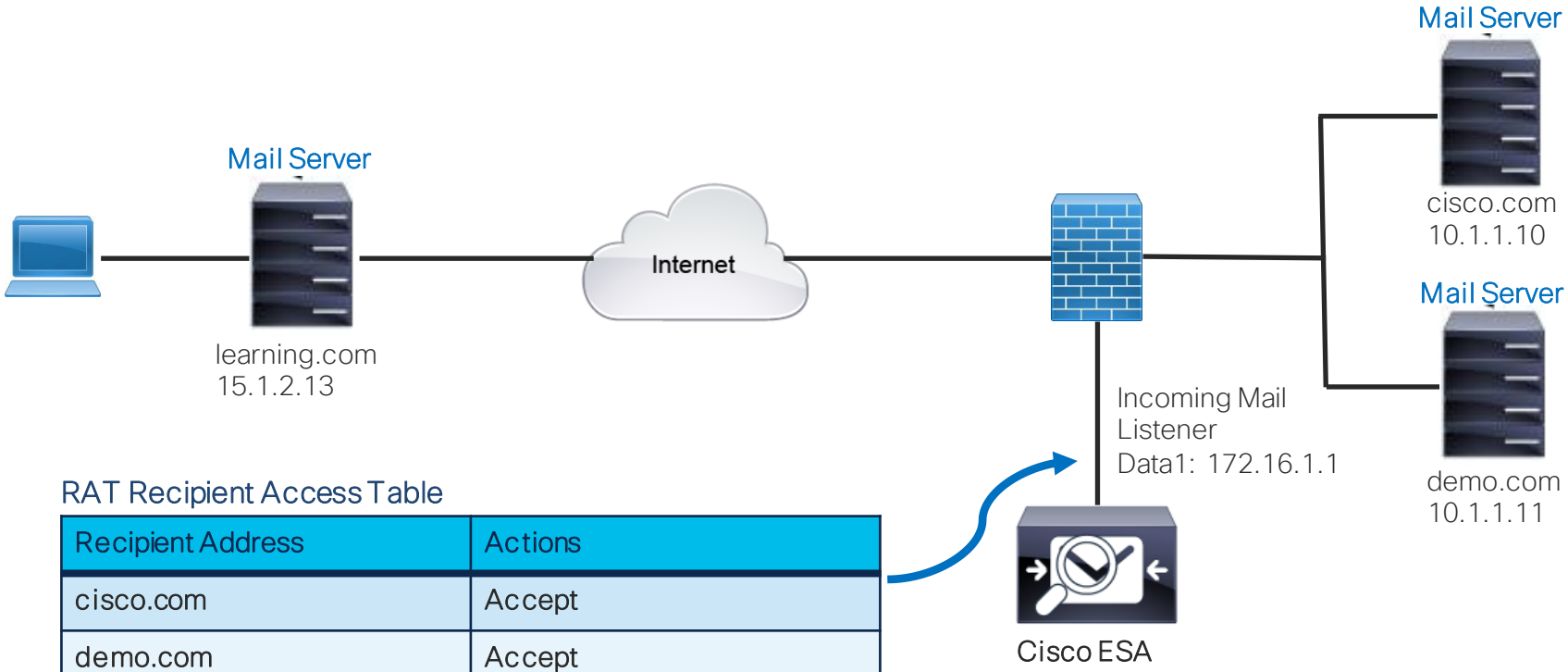
Déploiement deux interfaces HAT



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

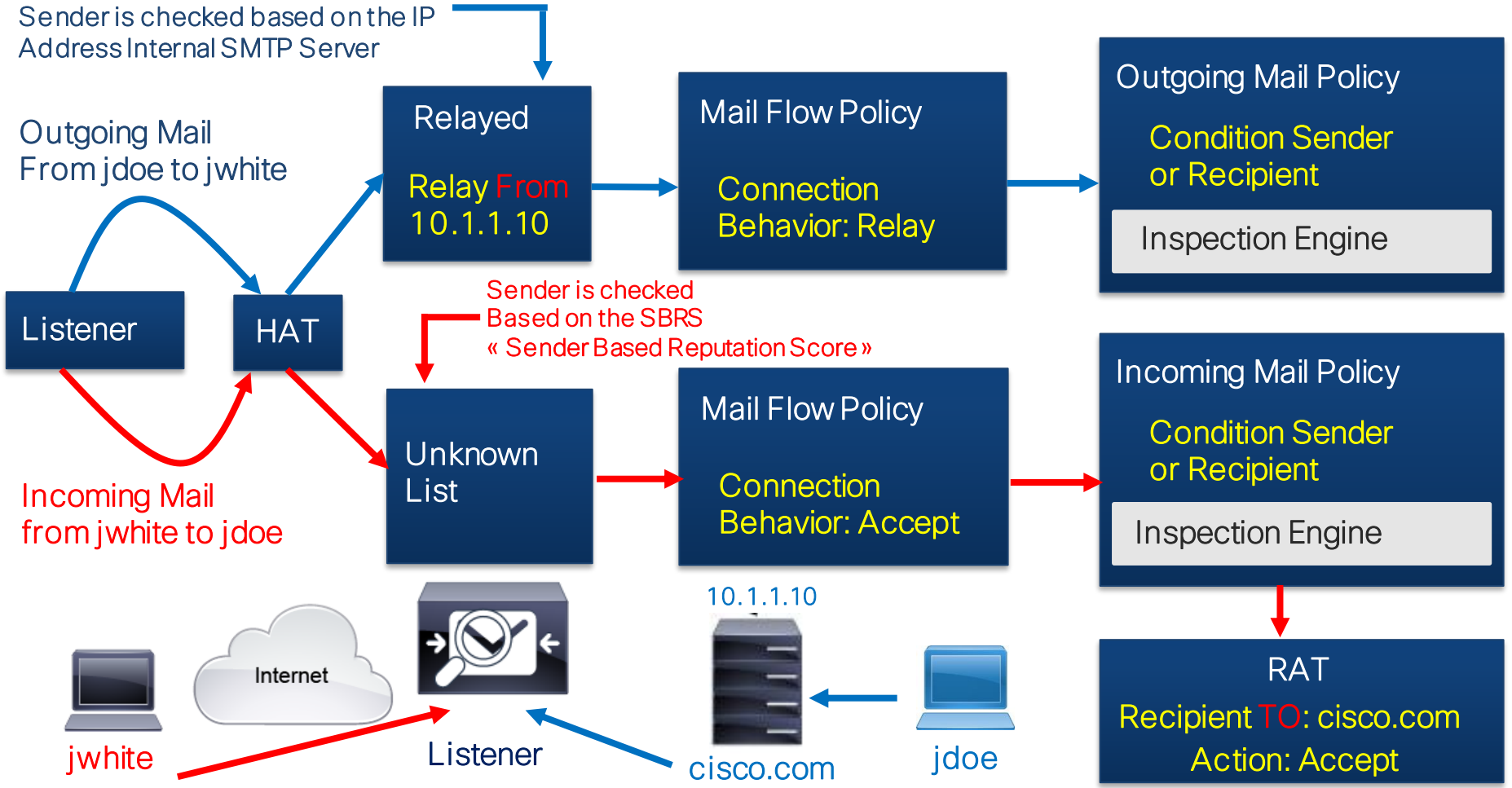
Déploiement deux interfaces RAT



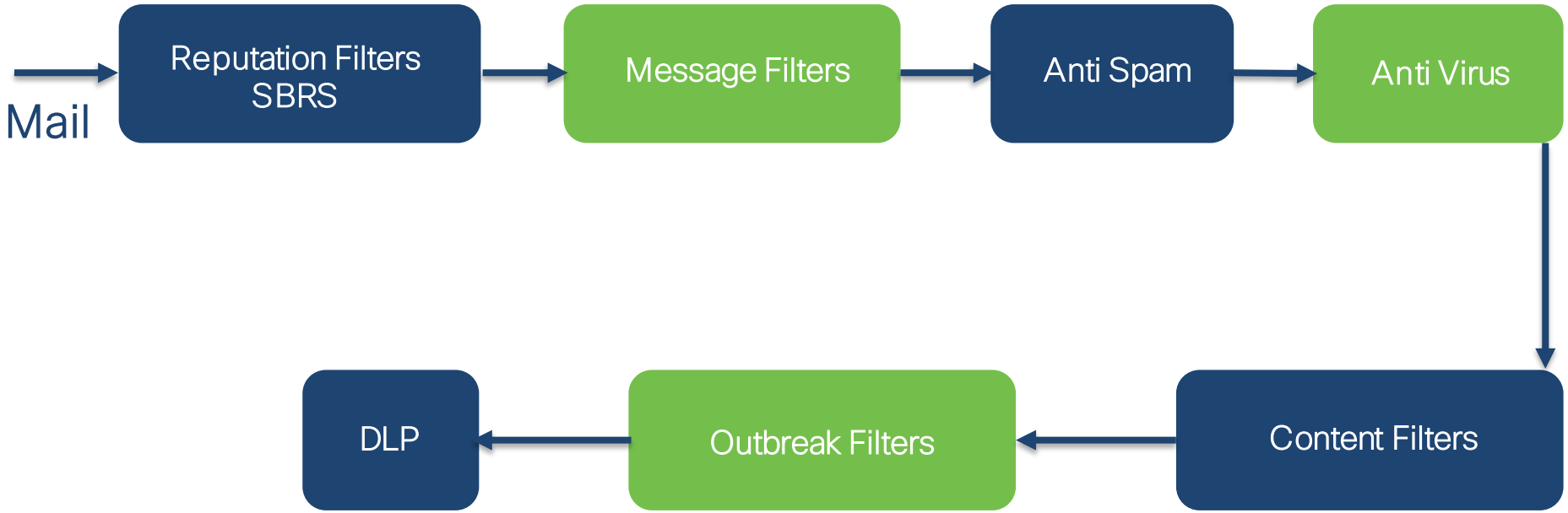
RAT Recipient Access Table

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

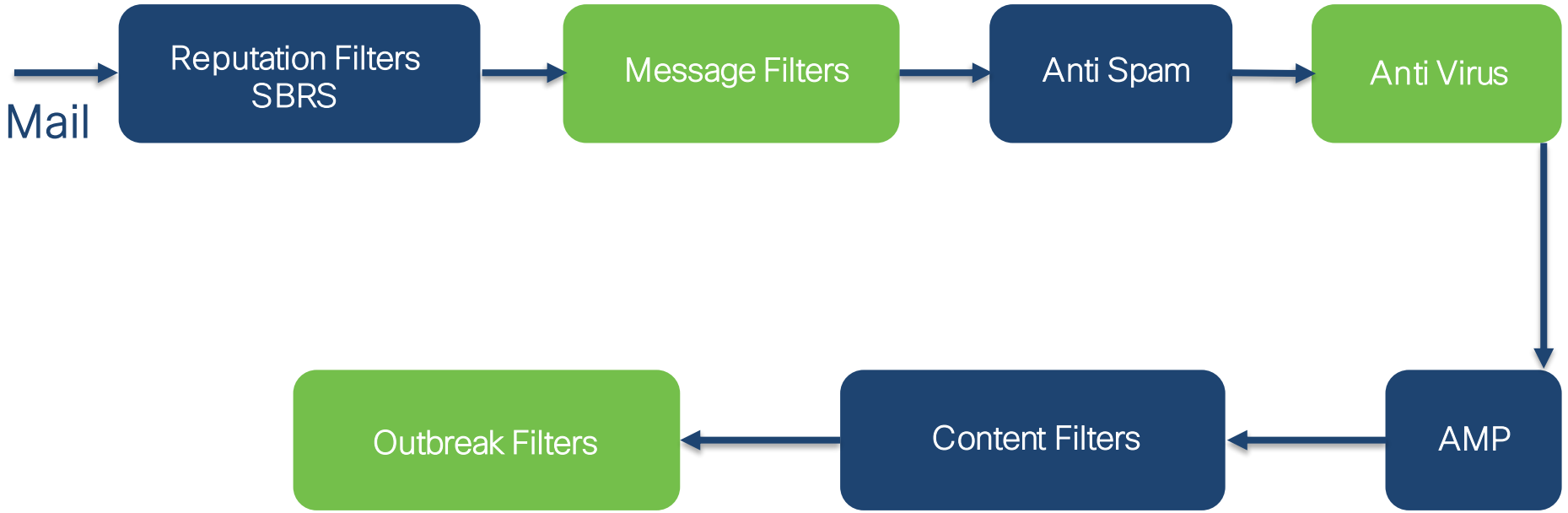
Mail Flow


Sender is checked based on the IP Address Internal SMTP Server
Outgoing Mail
From jdoe to jwhite
Relayed
Relay From 10.1.1.10
Mail Flow Policy
Connection Behavior: Relay
Outgoing Mail Policy
Condition Sender or Recipient
Inspection Engine
Listener
HAT
Sender is checked
Based on the SBRS
« Sender Based Reputation Score »
Unknown List
Mail Flow Policy
Connection Behavior: Accept
Incoming Mail Policy
Condition Sender or Recipient
Inspection Engine
Incoming Mail
from jwhite to jdoe
10.1.1.10
Internet
jwhite
Listener
cisco.com
jdoe
RAT
Recipient TO: cisco.com
Action: Accept

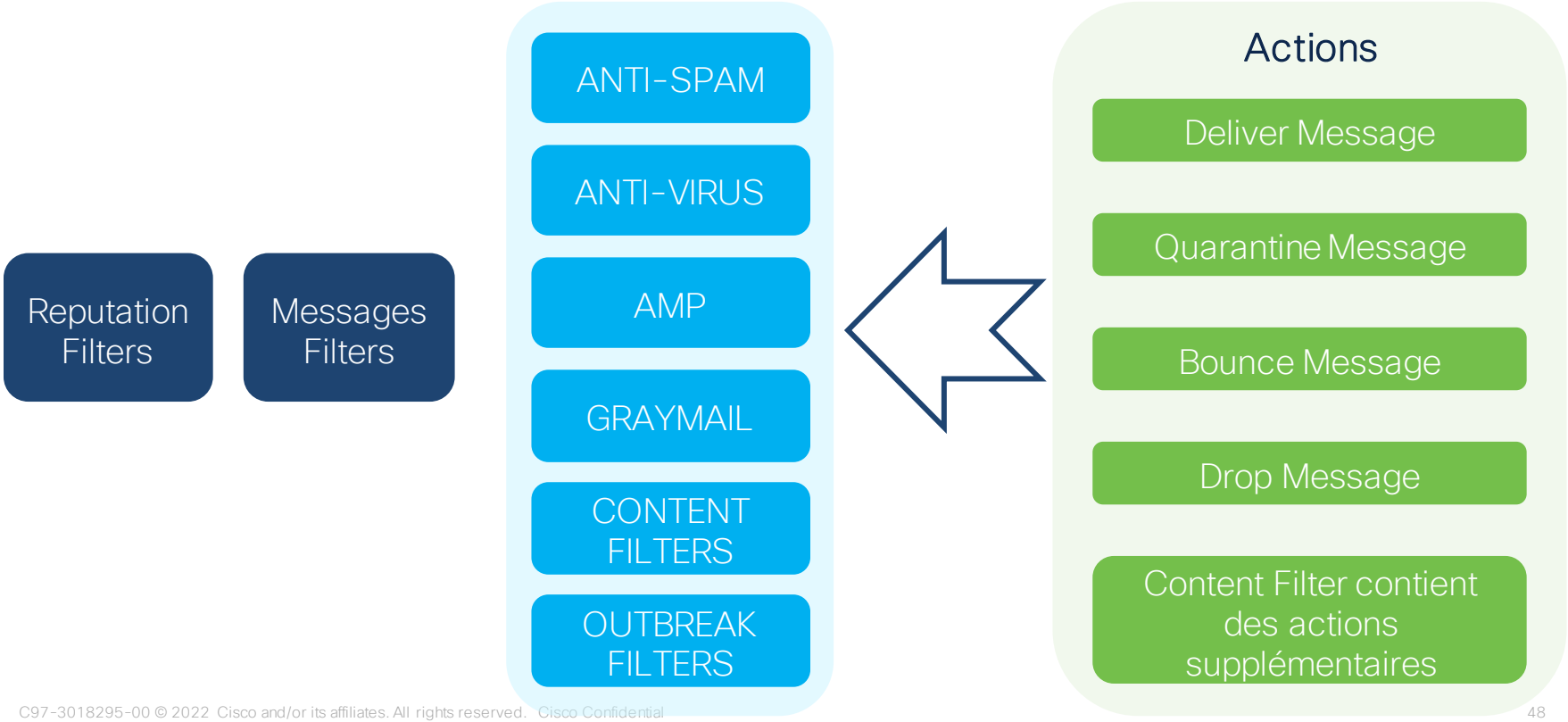
Outgoing Email Flow (Inspection Engine)



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