

BGP Blackholing Attack Defense

Loïc Miller

Supervised by Cristel PELSSER and Stéphane CATELOIN
18 janvier 2019



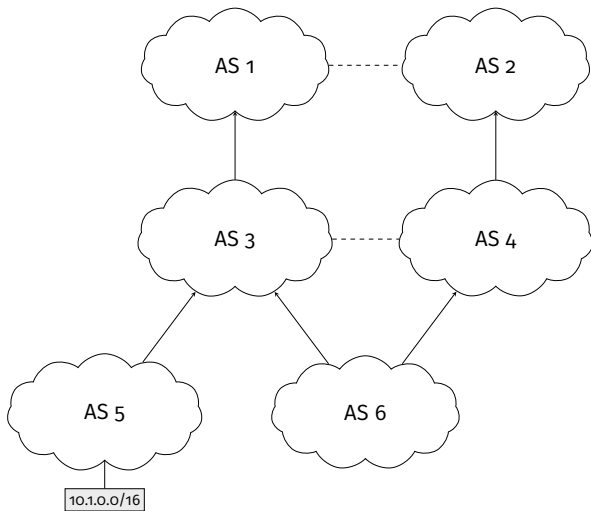


Figure 1: Propagation de messages BGP

¹Y. Rekhter, T. Li, and S. Hares. **A Border Gateway Protocol 4 (BGP-4)**. RFC 4271. RFC Editor, Jan. 2006. URL: <http://www.rfc-editor.org/rfc/rfc4271.txt>.

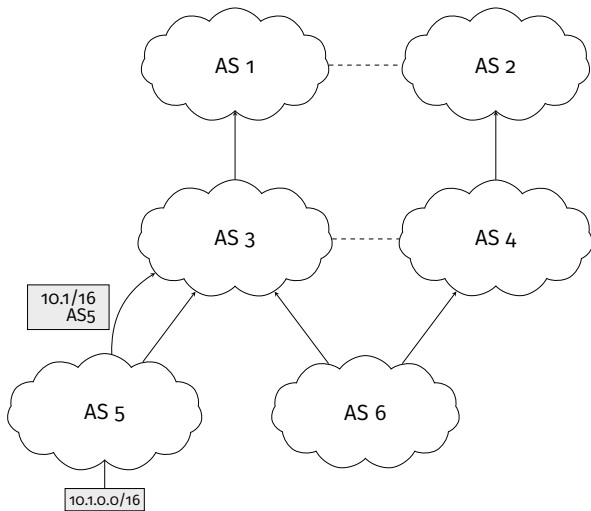


Figure 1: Propagation de messages BGP

¹Rekhter, Li, and Hares, **A Border Gateway Protocol 4 (BGP-4)**.

BGP - BORDER GATEWAY PROTOCOL¹

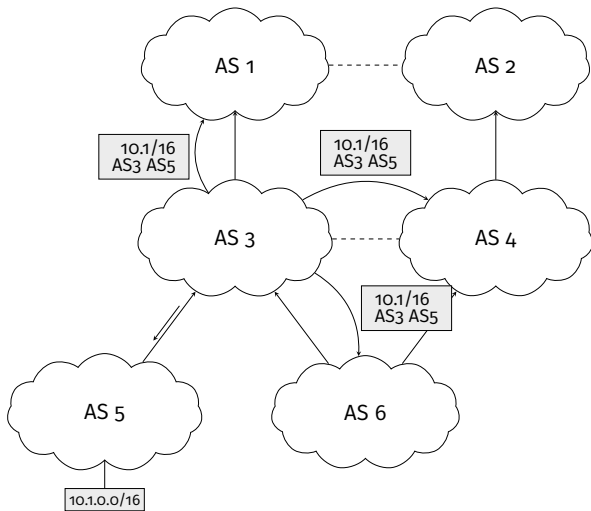


Figure 1: Propagation de messages BGP

¹Rekhter, Li, and Hares, **A Border Gateway Protocol 4 (BGP-4)**.

BGP - BORDER GATEWAY PROTOCOL¹

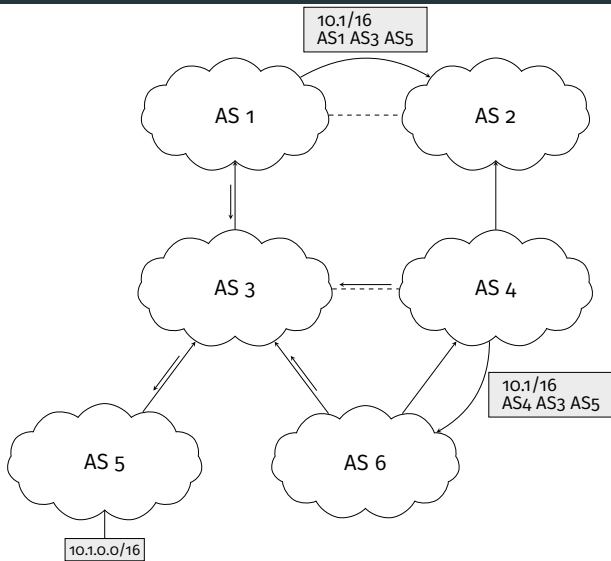


Figure 1: Propagation de messages BGP

¹Rekhter, Li, and Hares, **A Border Gateway Protocol 4 (BGP-4)**.

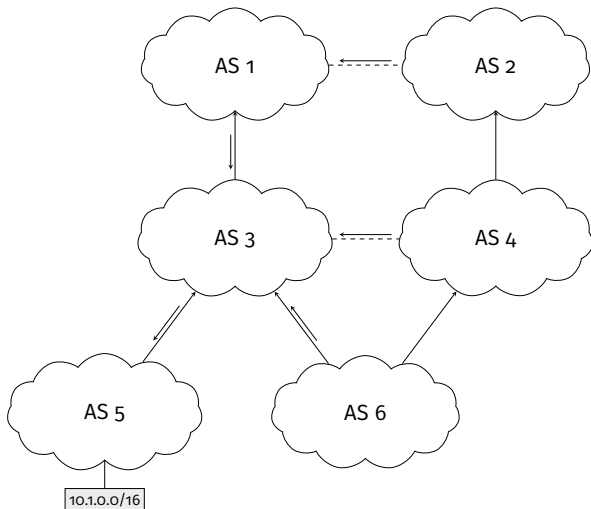


Figure 1: Propagation de messages BGP

¹Rekhter, Li, and Hares, **A Border Gateway Protocol 4 (BGP-4)**.

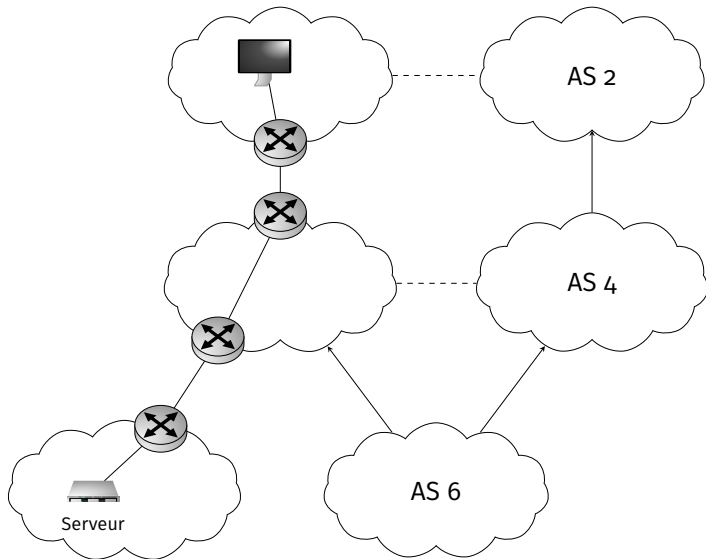


Figure 2: Attaque par déni de service

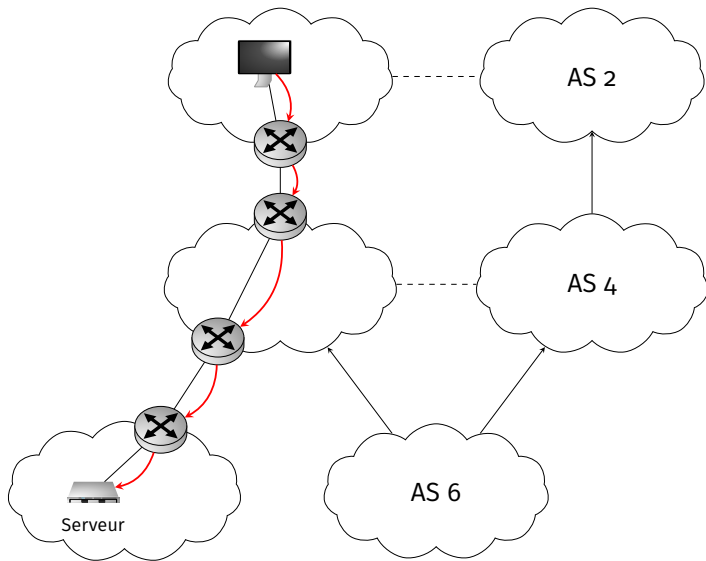


Figure 2: Attaque par déni de service

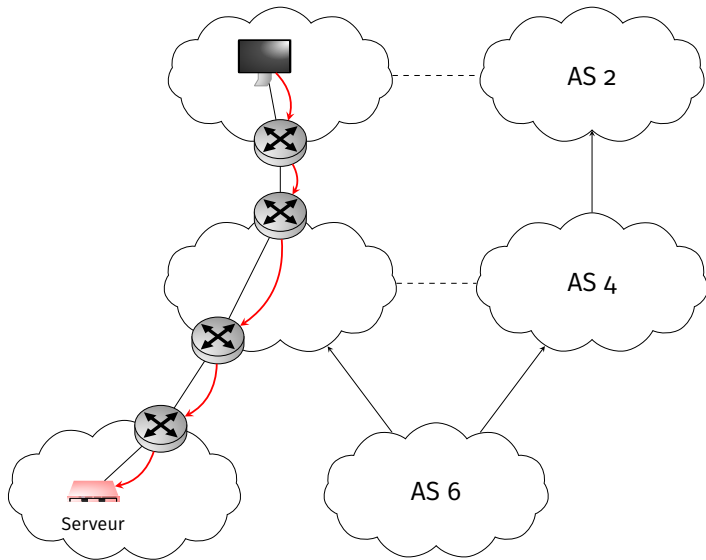


Figure 2: Attaque par déni de service

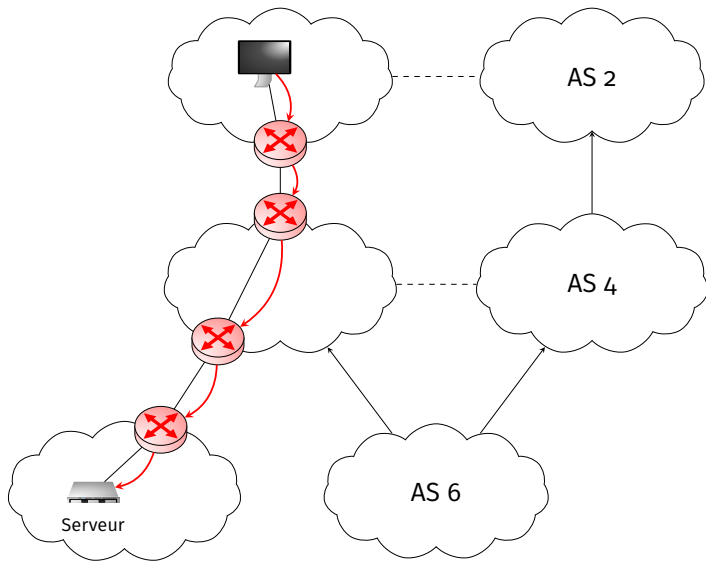


Figure 2: Attaque par déni de service

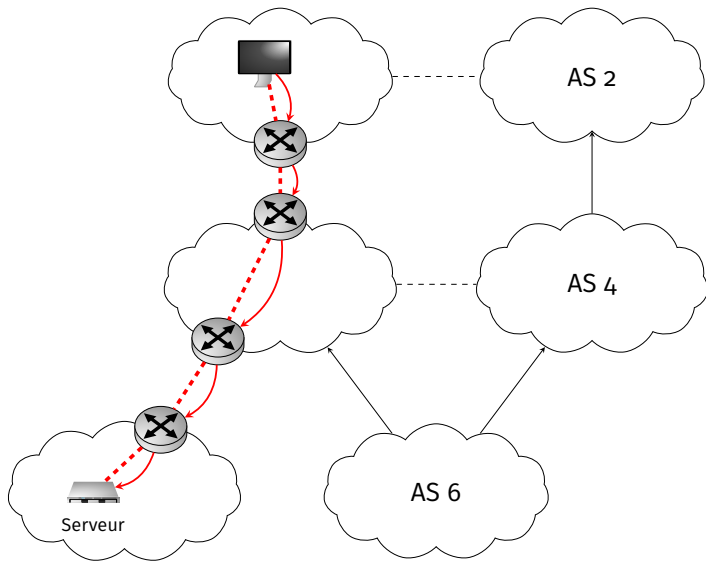


Figure 2: Attaque par déni de service

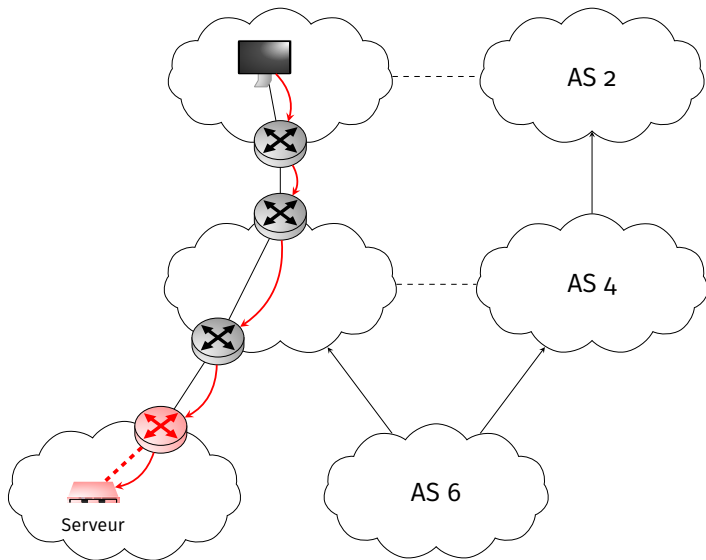


Figure 2: Attaque par déni de service

DDOS - ATTAQUES PAR DÉNI DE SERVICE DISTRIBUÉ

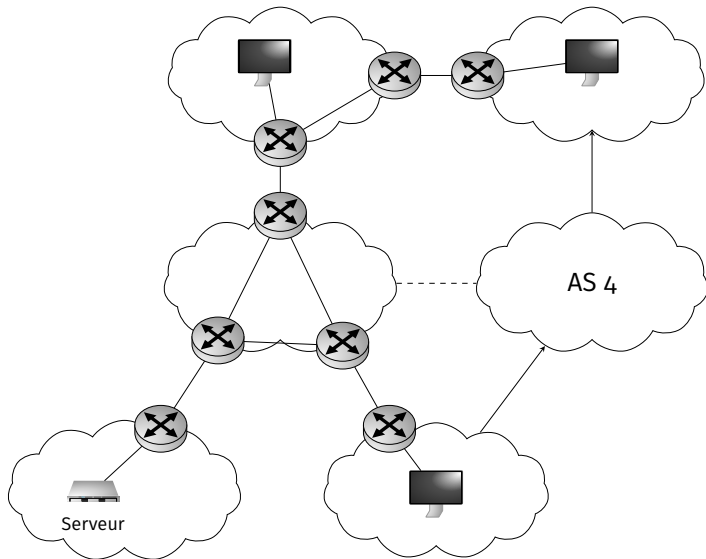


Figure 3: Attaque par déni de service distribué

DDOS - ATTAQUES PAR DÉNI DE SERVICE DISTRIBUÉ

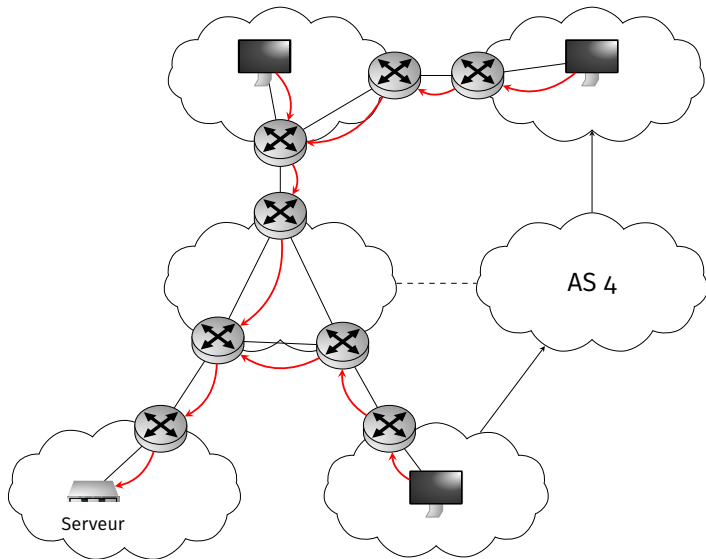


Figure 3: Attaque par déni de service distribué

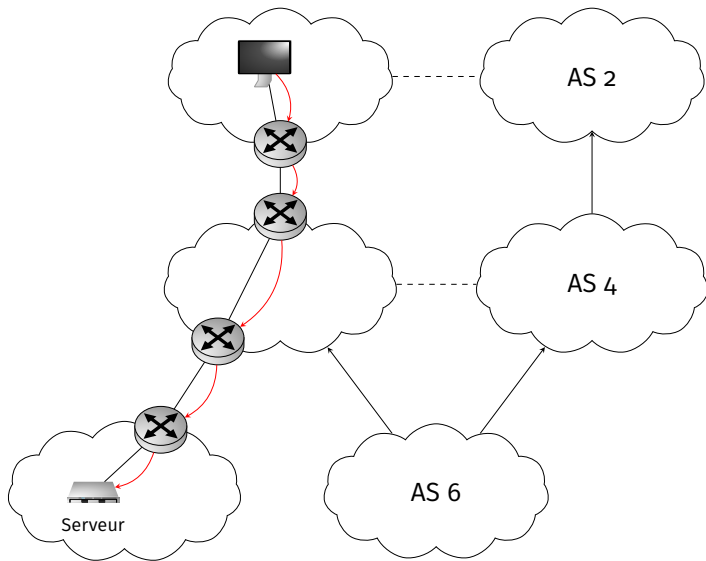


Figure 4: Mitigation par blackholing

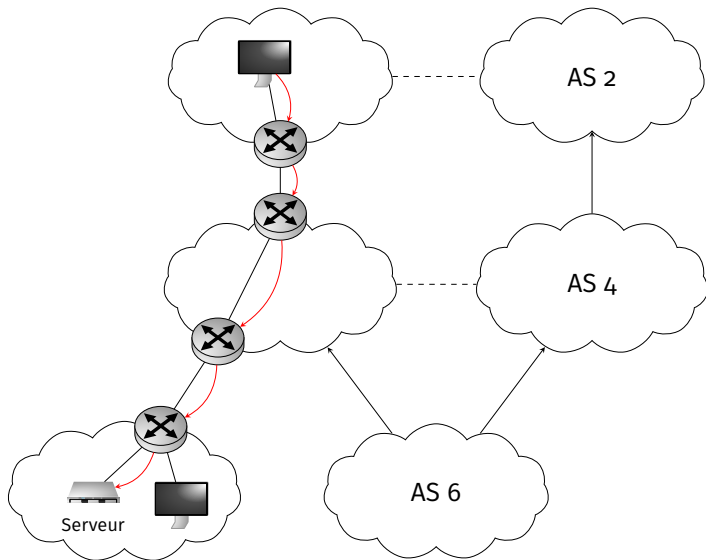


Figure 4: Mitigation par blackholing

BLACKHOLING - UNE TECHNIQUE DE MITIGATION

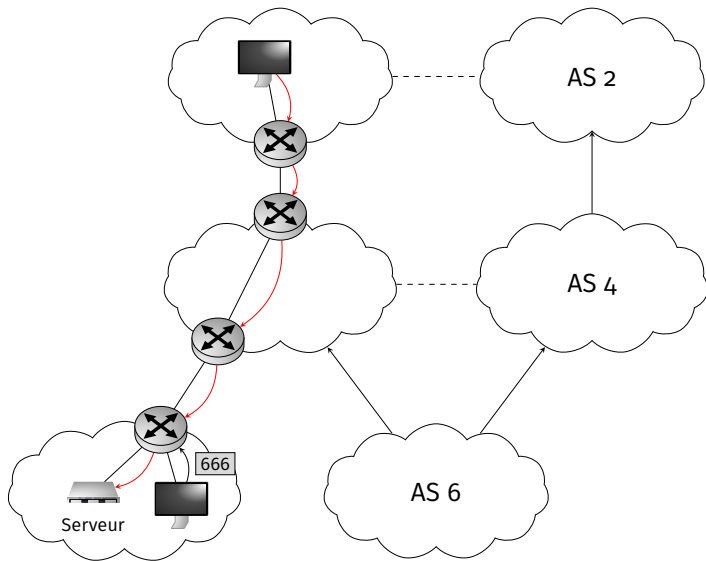


Figure 4: Mitigation par blackholing

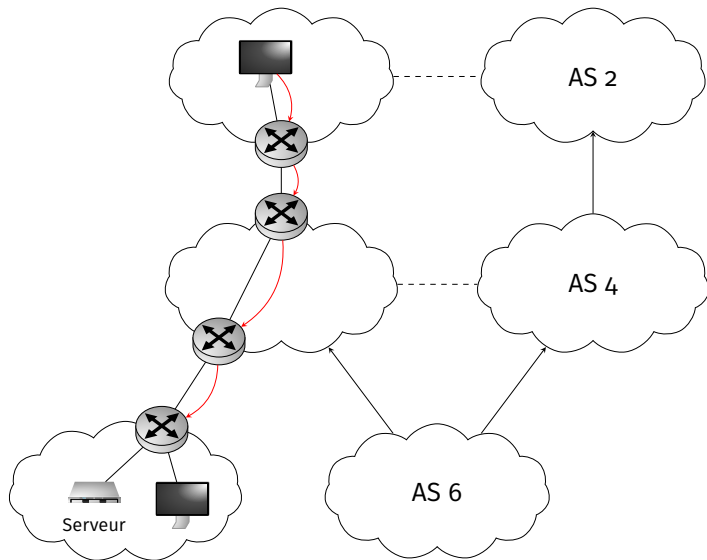


Figure 4: Mitigation par blackholing

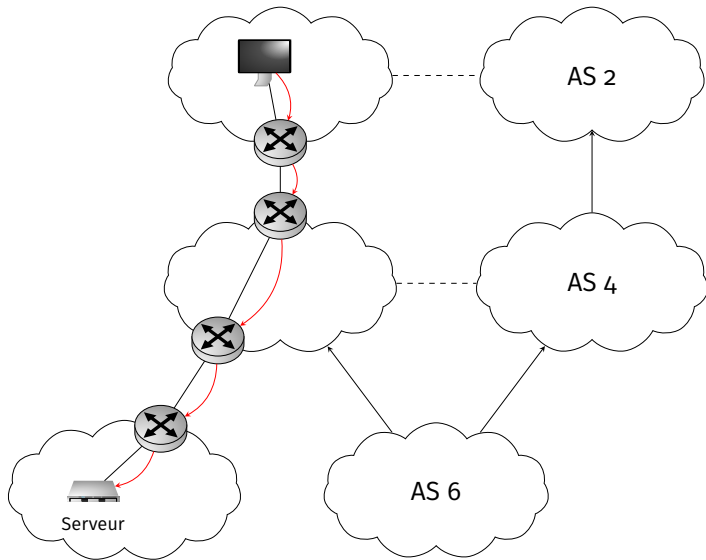


Figure 5: Mitigation par blackholing

BLACKHOLING - UNE TECHNIQUE DE MITIGATION

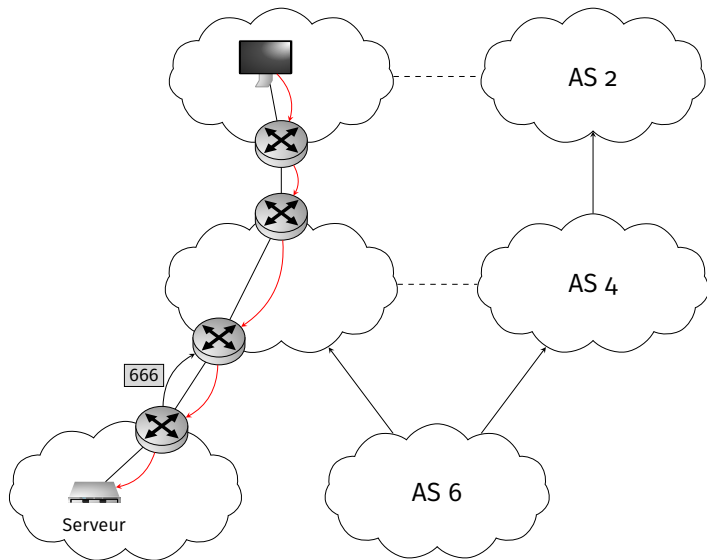


Figure 5: Mitigation par blackholing

BLACKHOLING - UNE TECHNIQUE DE MITIGATION

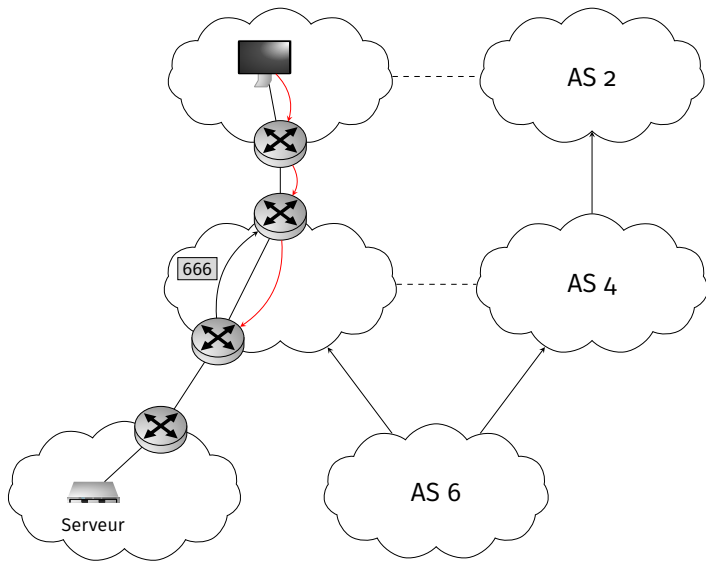


Figure 5: Mitigation par blackholing

BLACKHOLING - UNE TECHNIQUE DE MITIGATION

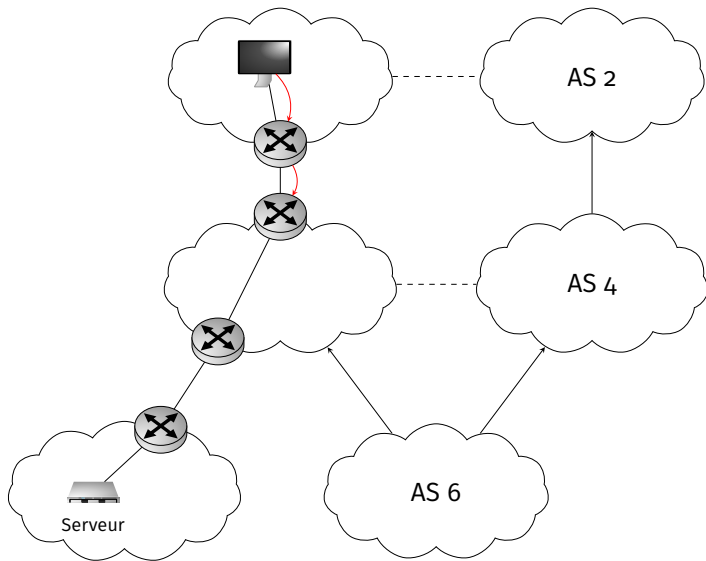


Figure 5: Mitigation par blackholing

- Peut-on utiliser le blackholing à mauvais escient?

- Peut-on utiliser le blackholing à mauvais escient?
- Types d'attaques possibles?

- Peut-on utiliser le blackholing à mauvais escient?
- Types d'attaques possibles?
- Mesures de protections existantes?

- Peut-on utiliser le blackholing à mauvais escient?
- Types d'attaques possibles?
- Mesures de protections existantes? Sont-elles suffisantes?

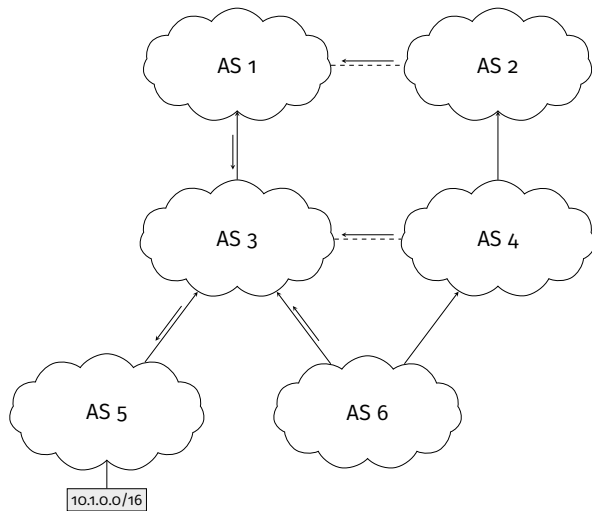


Figure 6: Hijack d'un préfixe

²Pavlos Sermpezis et al. "ARTEMIS: Neutralizing BGP Hijacking within a Minute". In: [arXiv preprint arXiv:1801.01085](#) (2018).

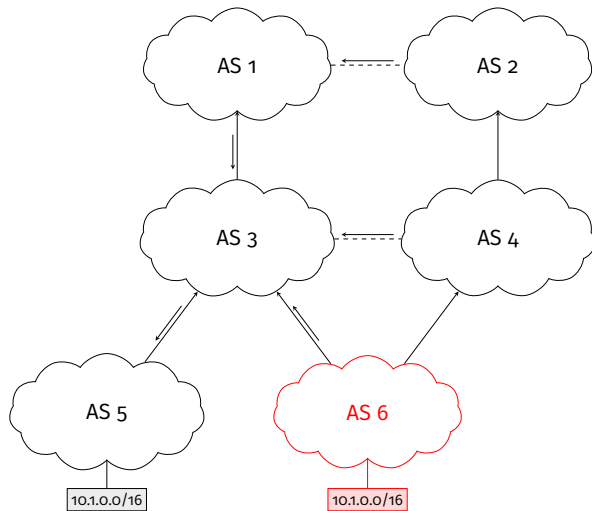


Figure 6: Hijack d'un préfixe

²Sermpetis et al., "ARTEMIS: Neutralizing BGP Hijacking within a Minute".

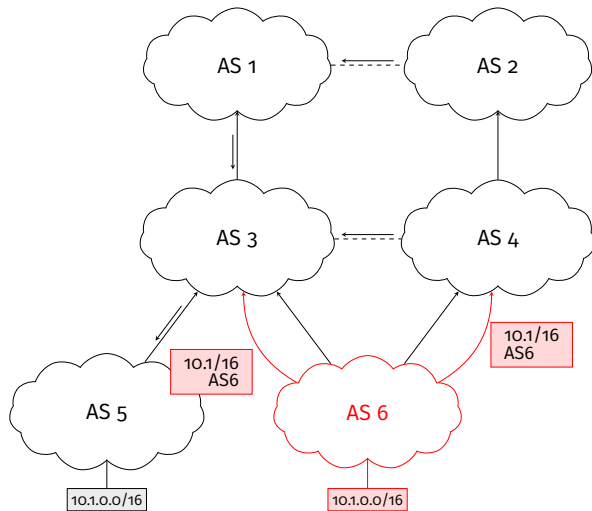


Figure 6: Hijack d'un préfixe

²Serpezis et al., "ARTEMIS: Neutralizing BGP Hijacking within a Minute".

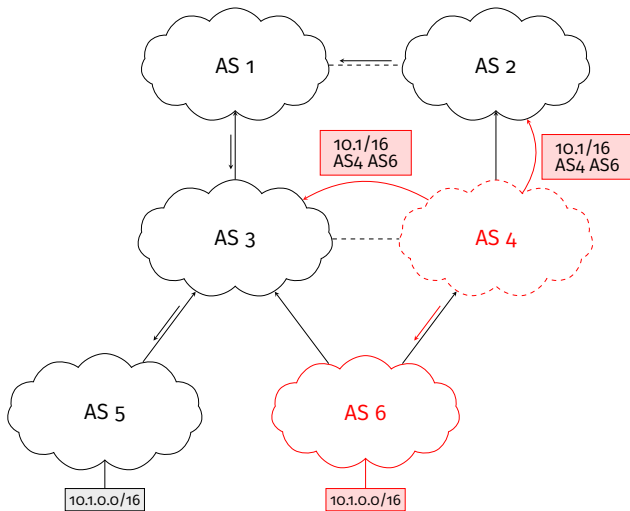


Figure 6: Hijack d'un préfixe

²Sermpetis et al., "ARTEMIS: Neutralizing BGP Hijacking within a Minute".

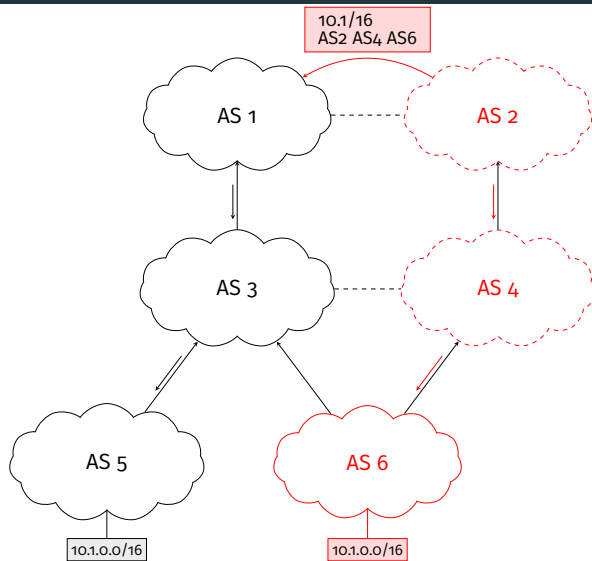


Figure 6: Hijack d'un préfixe

²Serpepezis et al., "ARTEMIS: Neutralizing BGP Hijacking within a Minute".

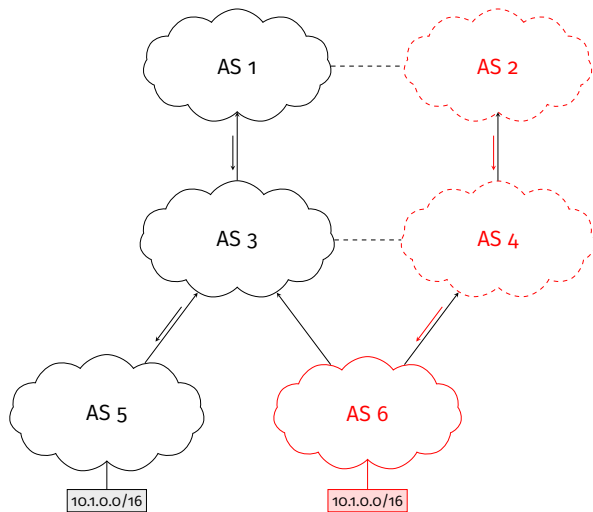


Figure 6: Hijack d'un préfixe

²Sermpetis et al., "ARTEMIS: Neutralizing BGP Hijacking within a Minute".

BGP BLACKHOLING (TYPE-O)

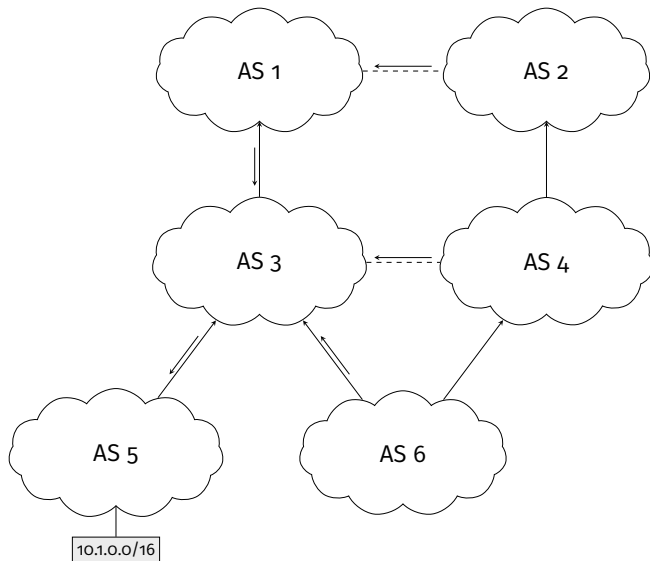


Figure 7: Blackhole d'un préfixe

BGP BLACKHOLING (TYPE-O)

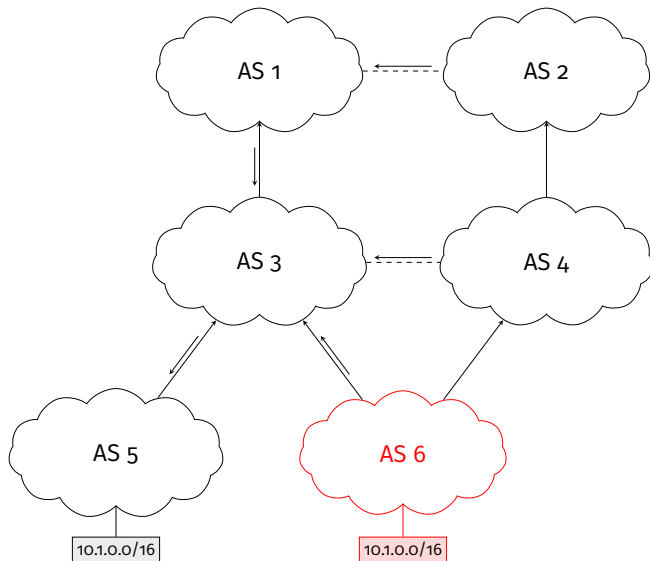


Figure 7: Blackhole d'un préfixe

BGP BLACKHOLING (TYPE-O)

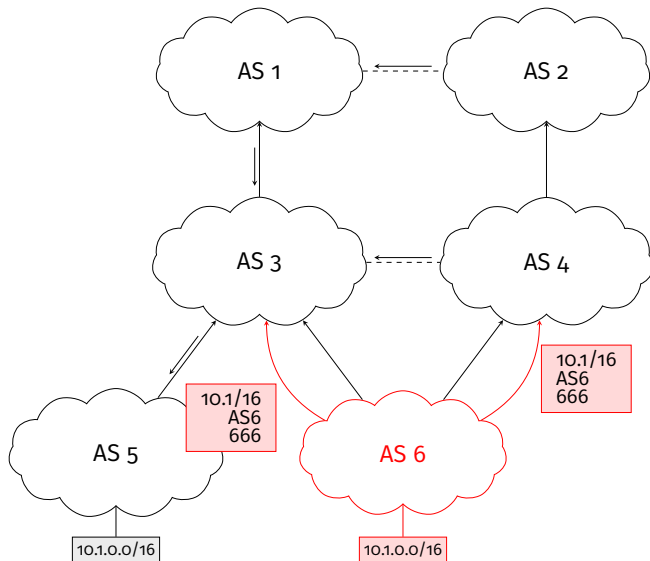


Figure 7: Blackhole d'un préfixe

BGP BLACKHOLING (TYPE-O)

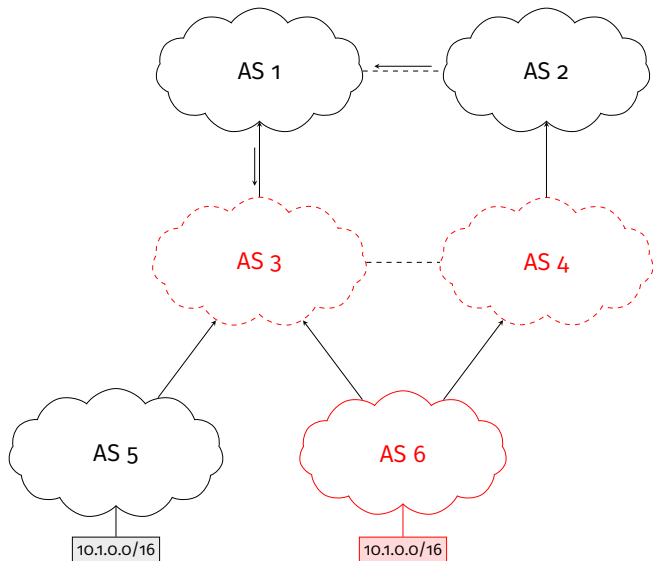


Figure 7: Blackhole d'un préfixe

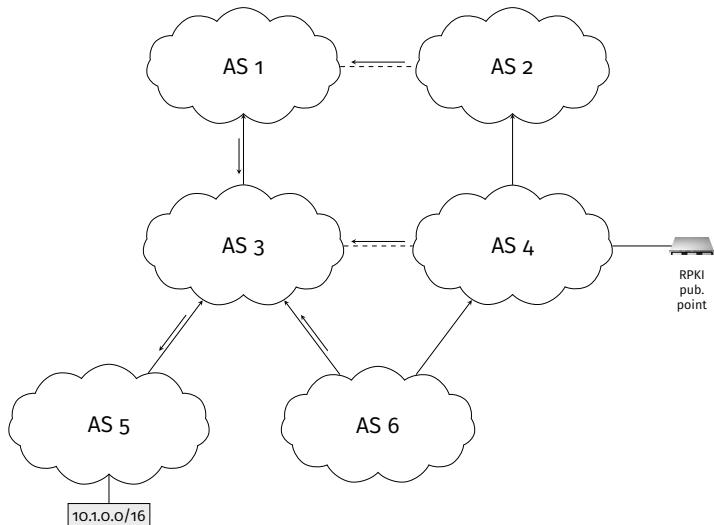


Figure 8: Utilisation de la RPKI

³M. Lepinski and S. Kent. **An Infrastructure to Support Secure Internet Routing**. RFC 6480. RFC Editor, Feb. 2012. URL: <http://www.rfc-editor.org/rfc/rfc6480.txt>.

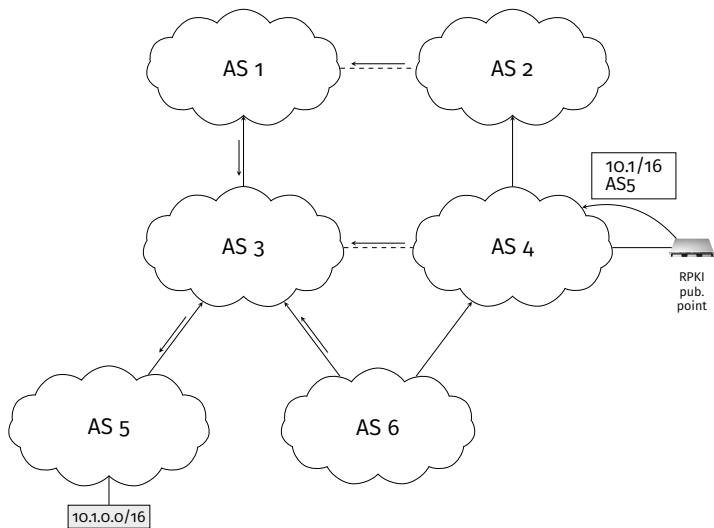


Figure 8: Utilisation de la RPKI

³Lepinski and Kent, **An Infrastructure to Support Secure Internet Routing**.

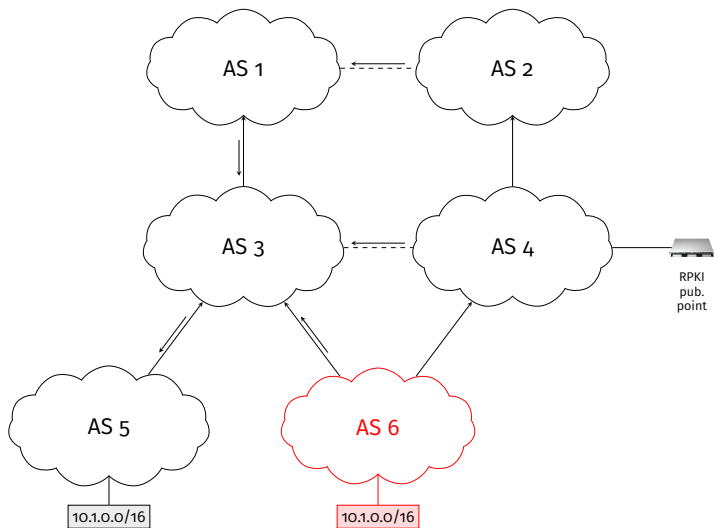


Figure 8: Utilisation de la RPKI

³Lepinski and Kent, **An Infrastructure to Support Secure Internet Routing**.

RPKI - RESOURCE PUBLIC KEY INFRASTRUCTURE³

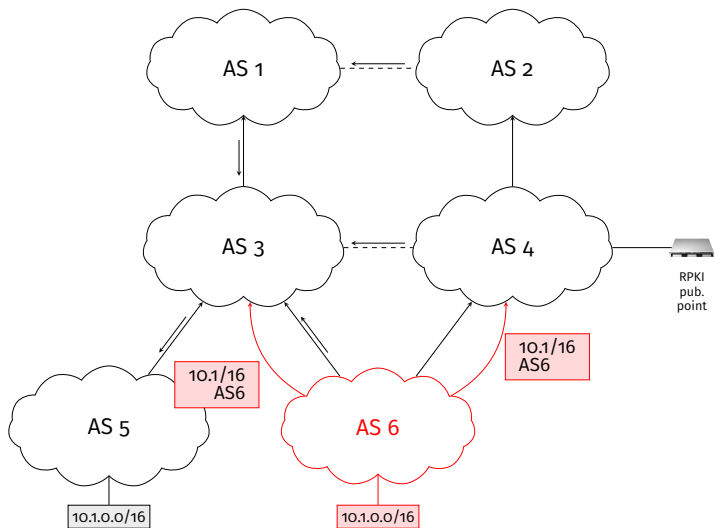


Figure 8: Utilisation de la RPKI

³Lepinski and Kent, **An Infrastructure to Support Secure Internet Routing**.

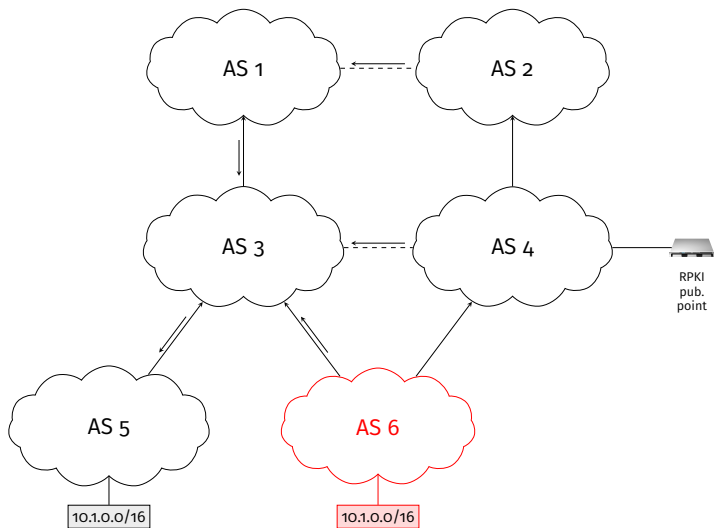


Figure 8: Utilisation de la RPKI

³Lepinski and Kent, **An Infrastructure to Support Secure Internet Routing**.

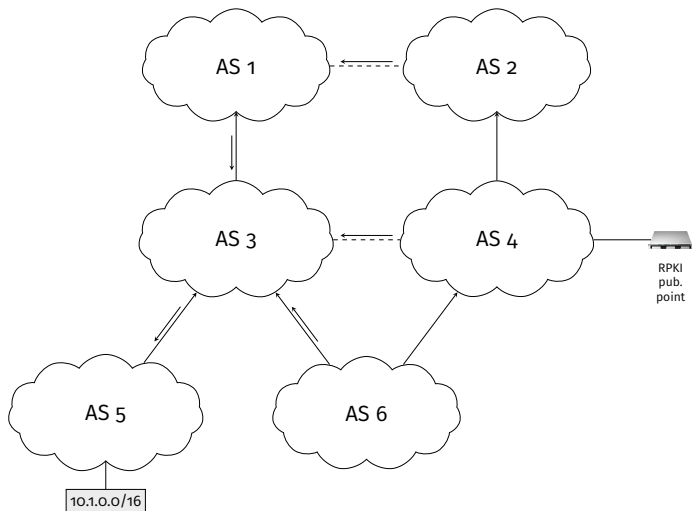


Figure 9: Hijack d'un préfixe

⁴Sermpezis et al., "ARTEMIS: Neutralizing BGP Hijacking within a Minute".

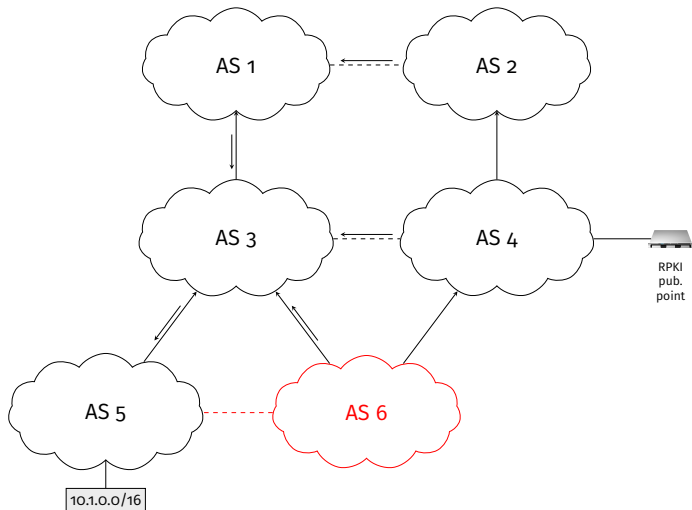


Figure 9: Hijack d'un préfixe

⁴Sermpezis et al., "ARTEMIS: Neutralizing BGP Hijacking within a Minute".

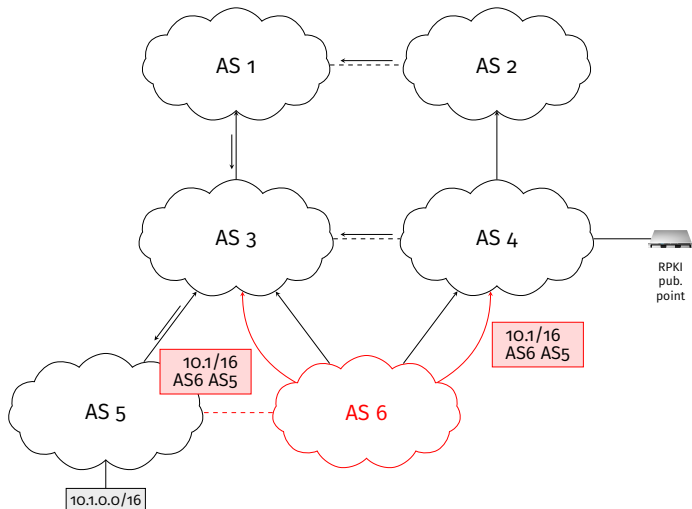


Figure 9: Hijack d'un préfixe

⁴Sermpezis et al., "ARTEMIS: Neutralizing BGP Hijacking within a Minute".

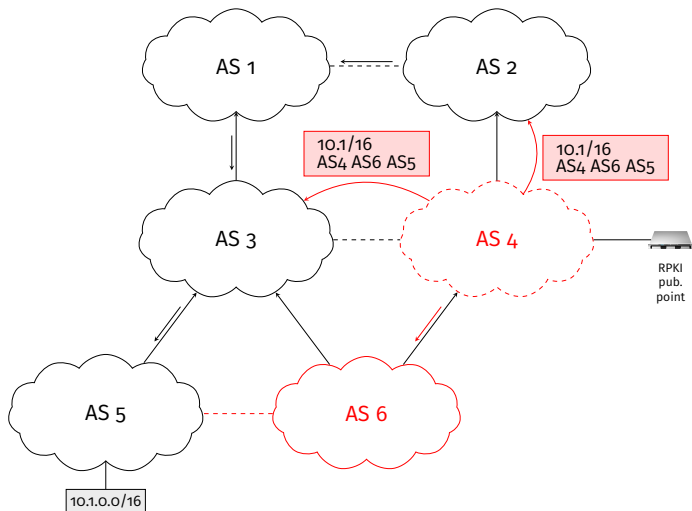


Figure 9: Hijack d'un préfixe

⁴Sermpezis et al., "ARTEMIS: Neutralizing BGP Hijacking within a Minute".

BGP HIJACKING REVISITED (TYPE-N)⁴

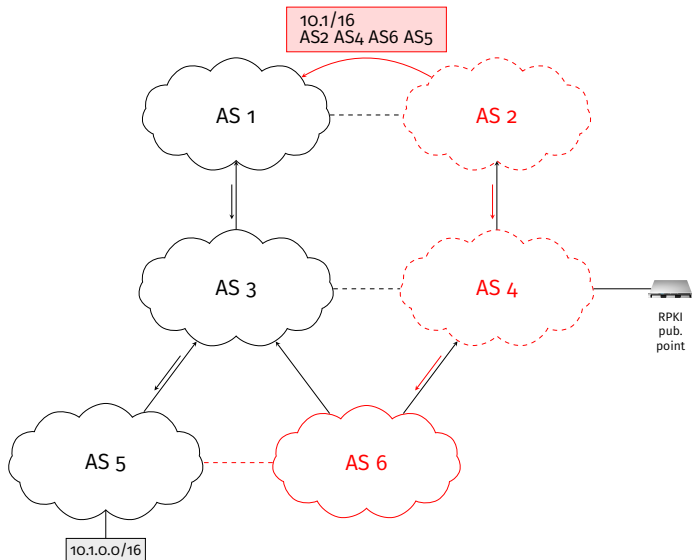


Figure 9: Hijack d'un préfixe

⁴Sermpezis et al., "ARTEMIS: Neutralizing BGP Hijacking within a Minute".

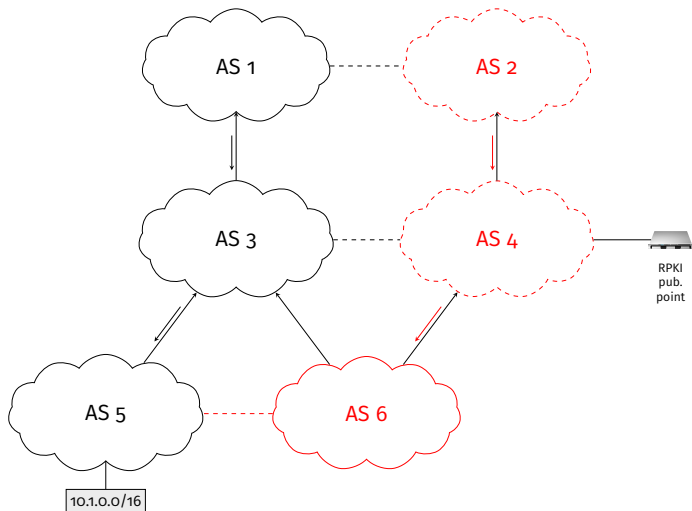


Figure 9: Hijack d'un préfixe

⁴Sermpezis et al., "ARTEMIS: Neutralizing BGP Hijacking within a Minute".

BGP BLACKHOLING REVISITED (TYPE-N)

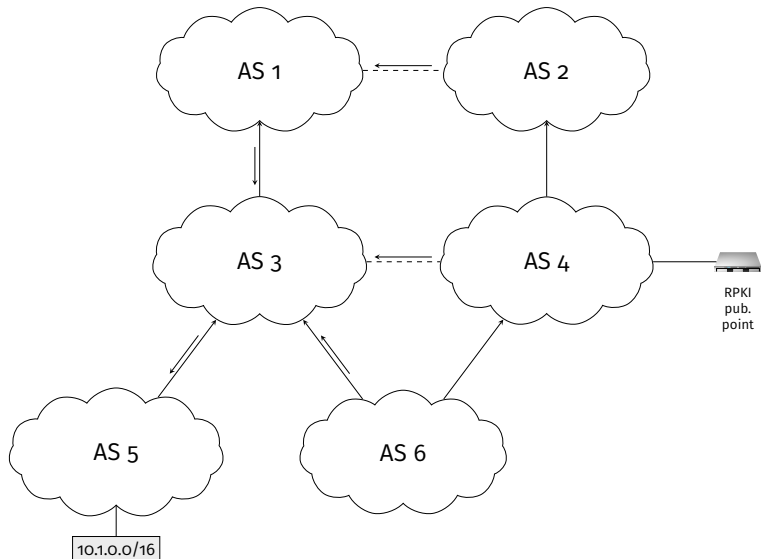


Figure 10: Blackhole d'un préfixe

BGP BLACKHOLING REVISITED (TYPE-N)

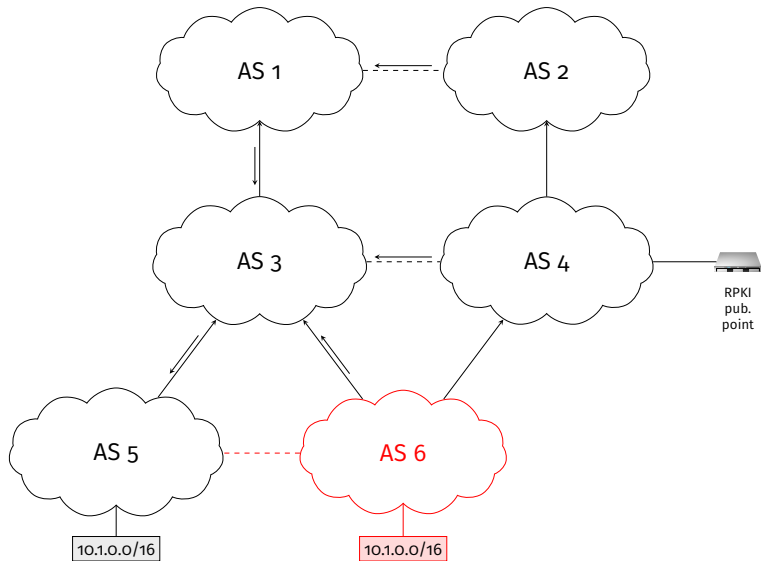


Figure 10: Blackhole d'un préfixe

BGP BLACKHOLING REVISITED (TYPE-N)

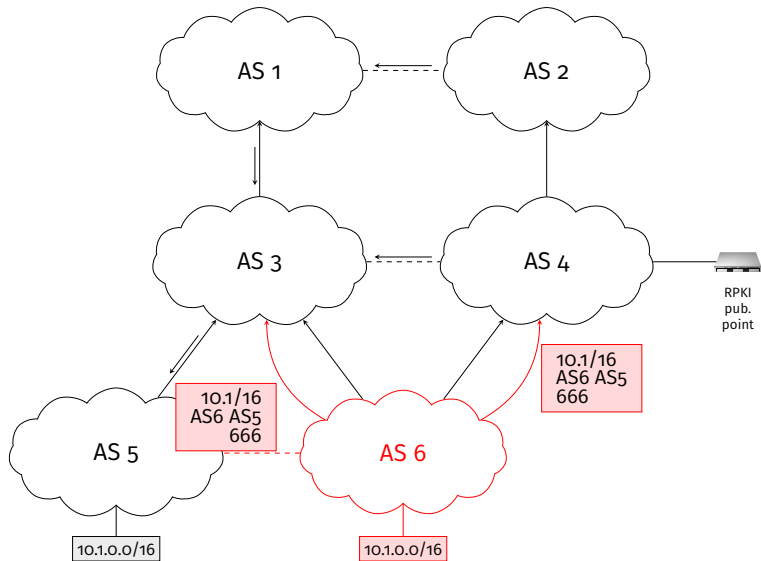


Figure 10: Blackhole d'un préfixe

BGP BLACKHOLING REVISITED (TYPE-N)

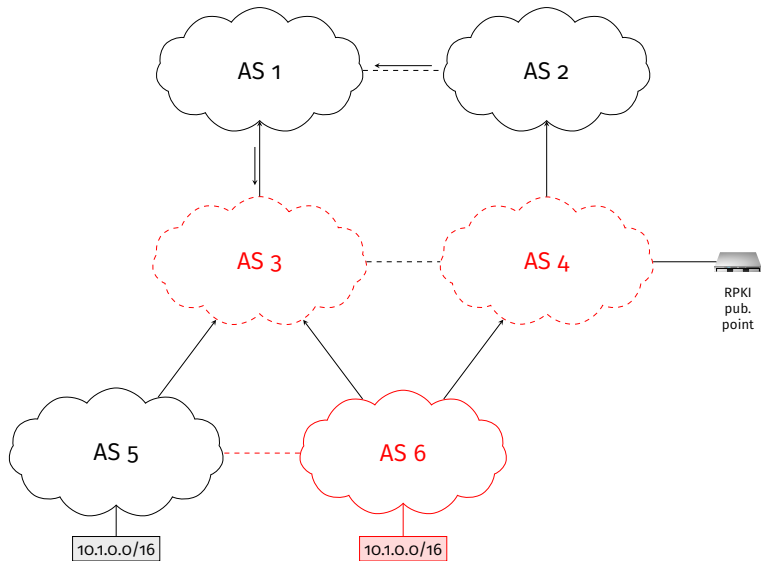


Figure 10: Blackhole d'un préfixe

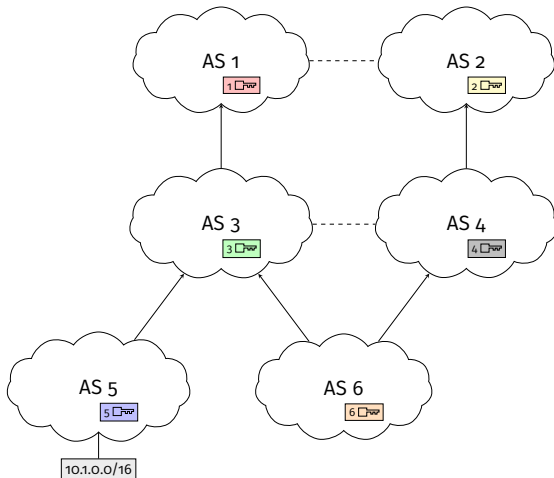


Figure 11: Propagation de messages BGPsec

⁵M. Lepinski and K. Sriram. **BGPsec Protocol Specification**. RFC 8205. RFC Editor, Sept. 2017.

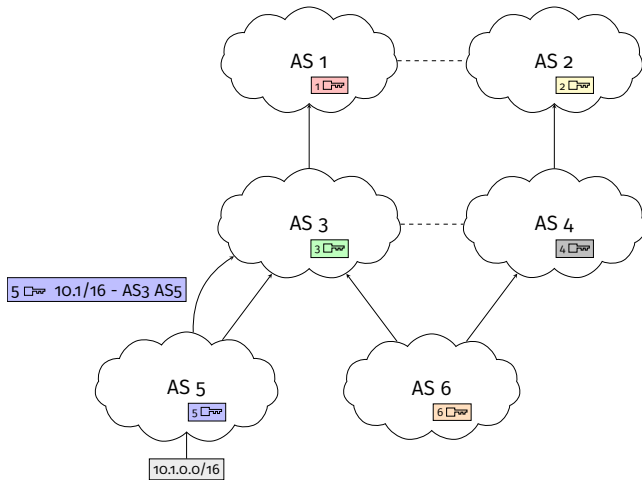


Figure 11: Propagation de messages BGPsec

⁵Lepinski and Sriram, **BGPsec Protocol Specification**.

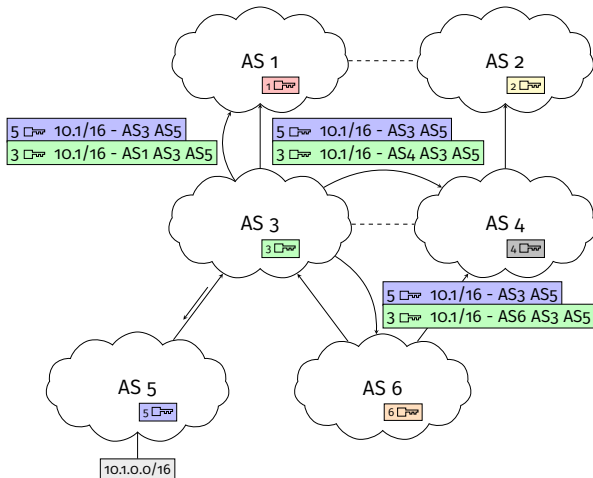


Figure 11: Propagation de messages BGPsec

⁵Lepinski and Sriram, **BGPsec Protocol Specification**.

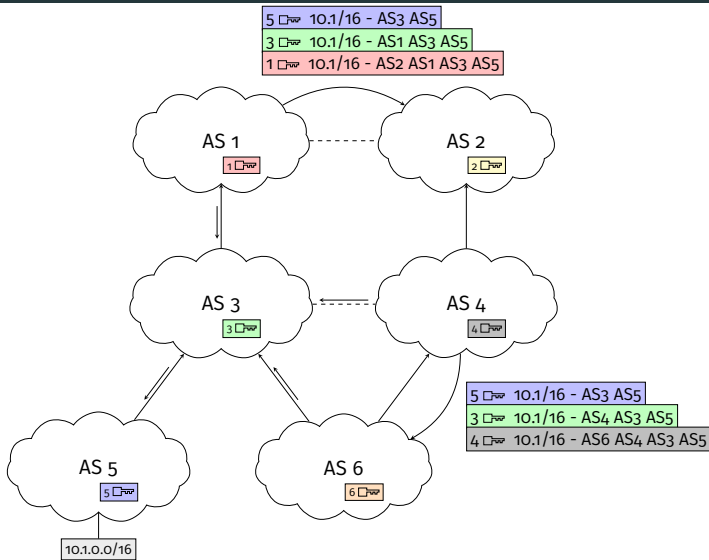


Figure 11: Propagation de messages BGPsec

⁵Lepinski and Sriram, **BGPsec Protocol Specification**.

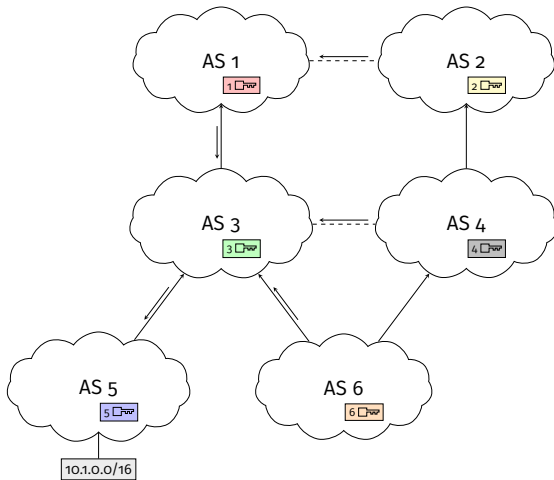


Figure 11: Propagation de messages BGPsec

⁵Lepinski and Sriram, **BGPsec Protocol Specification**.

BGP HIJACKING REVISITED (TYPE-N)⁶

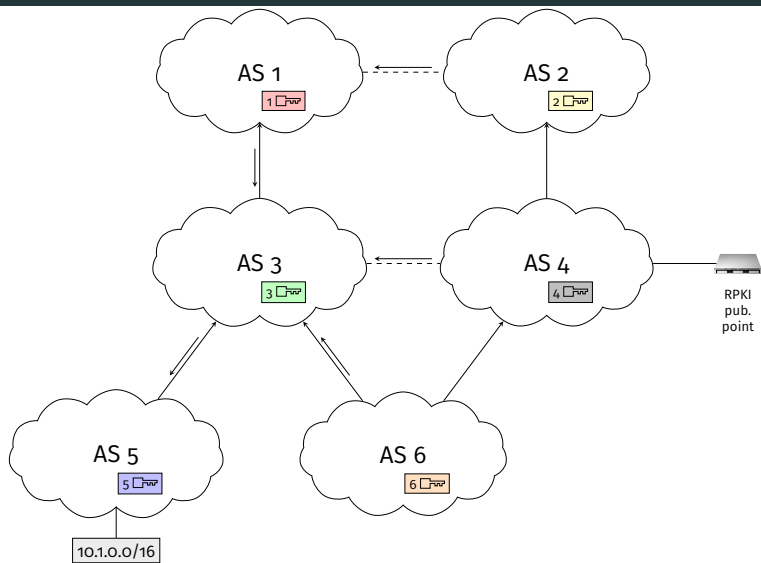


Figure 12: Hijack d'un préfixe

⁶Sermpezis et al., "ARTEMIS: Neutralizing BGP Hijacking within a Minute".

BGP HIJACKING REVISITED (TYPE-N)⁶

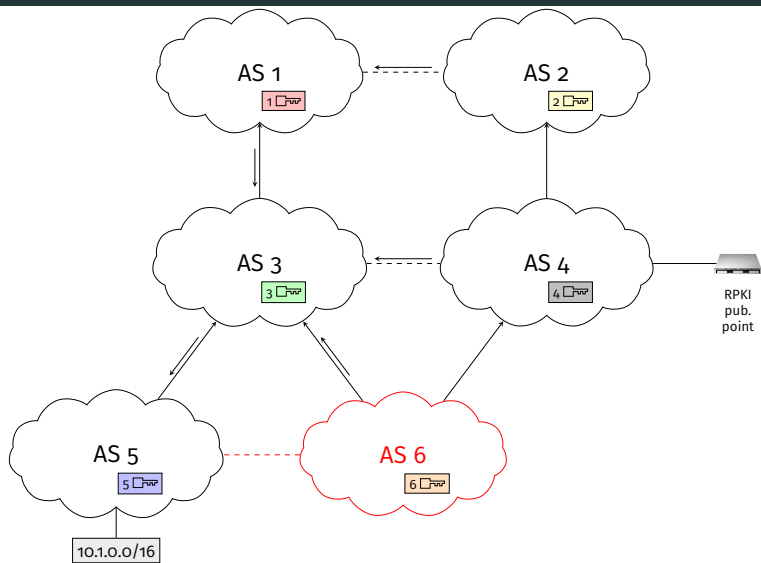


Figure 12: Hijack d'un préfixe

⁶Sermpezis et al., "ARTEMIS: Neutralizing BGP Hijacking within a Minute".

BGP HIJACKING REVISITED (TYPE-N)⁶

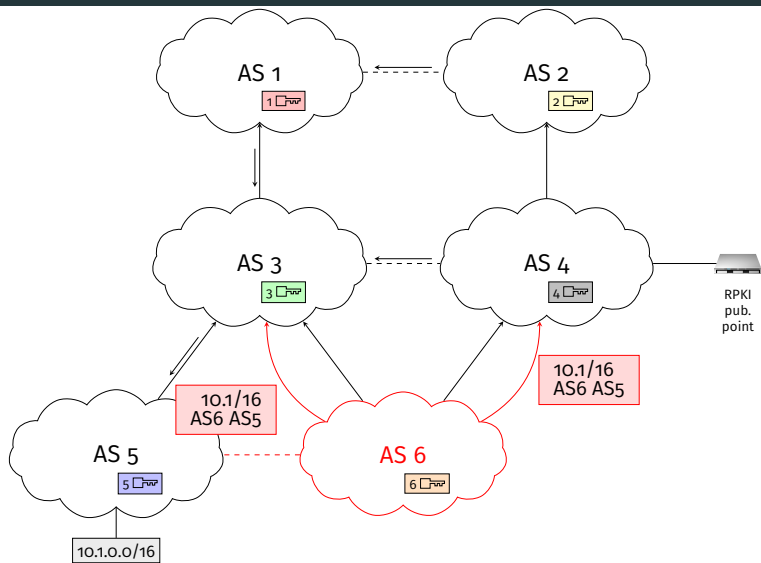


Figure 12: Hijack d'un préfixe

⁶Sermpezis et al., "ARTEMIS: Neutralizing BGP Hijacking within a Minute".

BGP HIJACKING REVISITED (TYPE-N)⁶

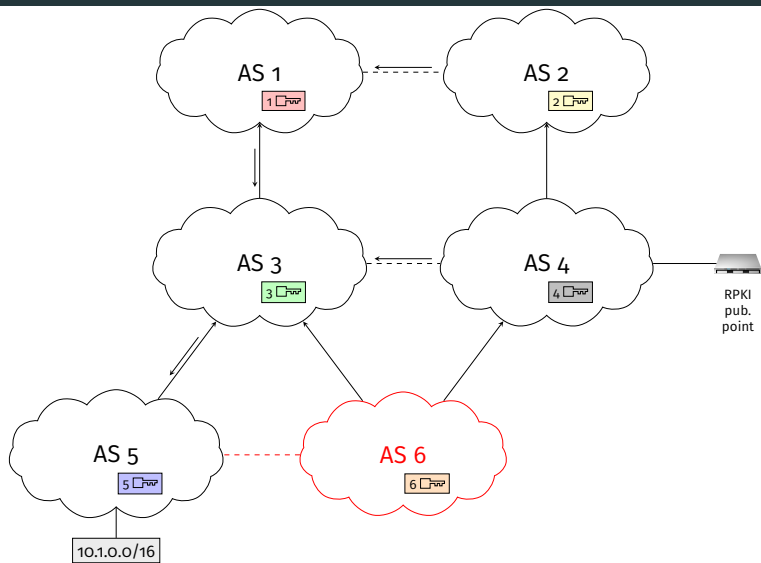


Figure 12: Hijack d'un préfixe

⁶Sermpezis et al., "ARTEMIS: Neutralizing BGP Hijacking within a Minute".

BGP BLACKHOLING REVISITED (ON PATH)

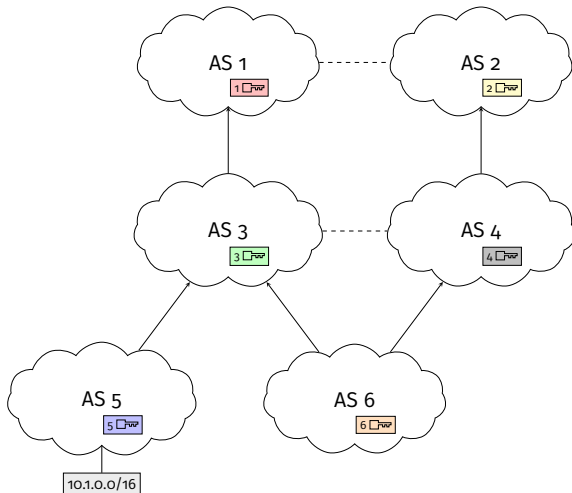


Figure 13: Blackhole d'un préfixe

BGP BLACKHOLING REVISITED (ON PATH)

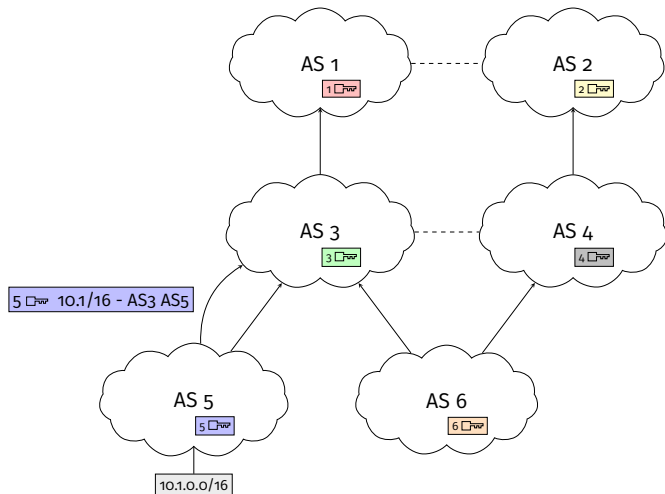


Figure 13: Blackhole d'un préfixe

BGP BLACKHOLING REVISITED (ON PATH)

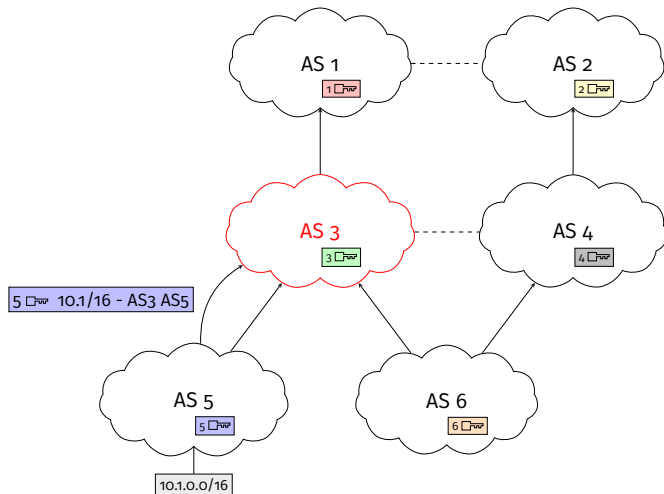


Figure 13: Blackhole d'un préfixe

BGP BLACKHOLING REVISITED (ON PATH)

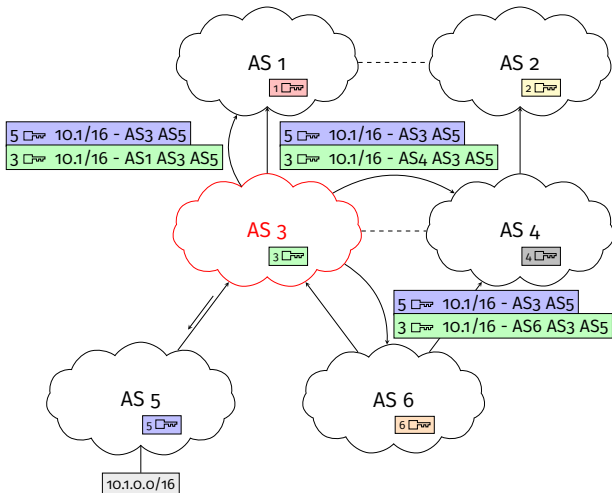


Figure 13: Blackhole d'un préfixe

BGP BLACKHOLING REVISITED (ON PATH)

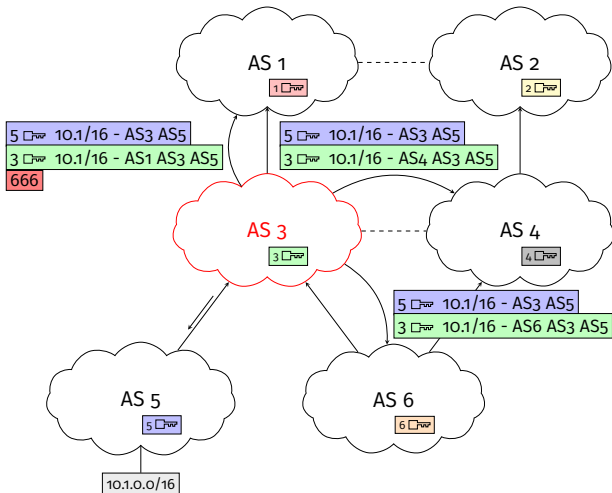


Figure 13: Blackhole d'un préfixe

BGP BLACKHOLING REVISITED (ON PATH)

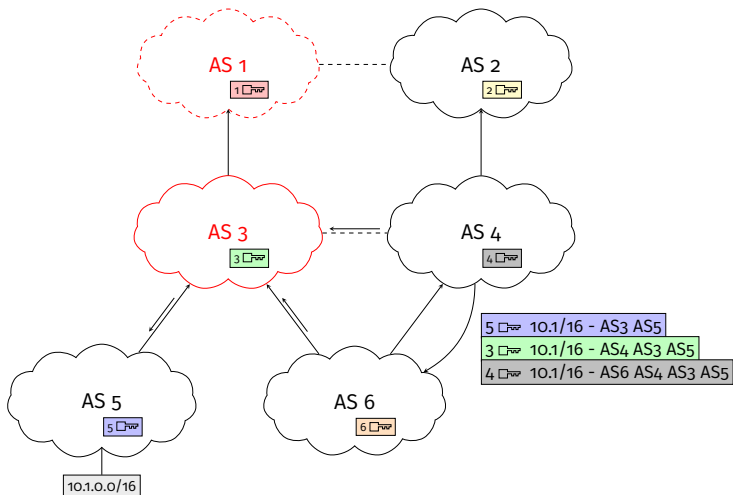


Figure 13: Blackhole d'un préfixe

BGP BLACKHOLING REVISITED (ON PATH)

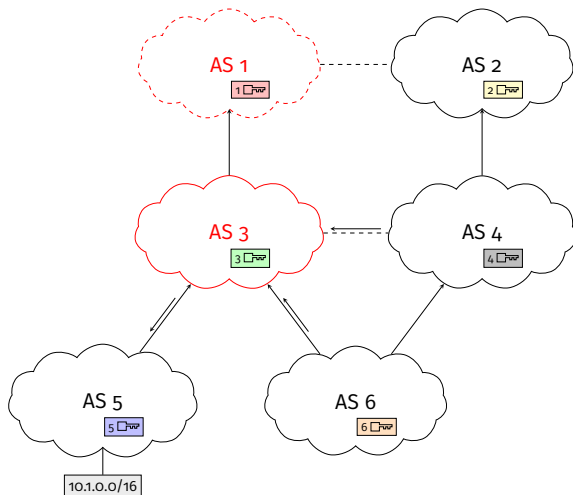


Figure 13: Blackhole d'un préfixe

Security Deployment	Hijack			On Path
	Type-o	Type-N	Type-U	
BGPsec (full)	✓	✓	✓	-
BGPsec (partial)	✓ / -	✓ / -	✓ / -	-
RPKI (full)	✓	-	-	-
RPKI (partial)	✓ / -	-	-	-
No security	-	-	-	-

Table 1: Sécurité des communautés contre les hijacks exacts

Security Deployment	Hijack		
	Type-o	Type-N	Type-U
BGPsec (full)	✓	✓	✓
BGPsec (partial)	✓ / -	✓ / -	✓ / -
RPKI (full)	✓	✓	✓
RPKI (partial)	✓ / -	✓ / -	✓ / -
No security	-	-	-

Table 2: Sécurité des communautés contre les hijacks de sous-préfixes

BONNES PRATIQUES POUR LE BLACKHOLING

	On Path	On Path (Infraction)	Hijack		
			Type-N	Type-U	Type-o
No rule	-	-	-	-	-
Legitimate peer	-	-	-	✓	-
RPKI	-	-	-	-	✓
BGPsec	-	-	✓	✓	-
Legitimate peer	-	-	-	✓	✓
RPKI	-	-	-	✓	✓
Legitimate peer	-	-	✓	✓	-
BGPsec	-	-	✓	✓	✓
Legitimate peer	-	-	✓	✓	✓
RPKI	-	-	✓	✓	✓
BGPsec	-	-	✓	✓	✓

Table 3: Protection assurée par les bonnes pratiques

BONNES PRATIQUES POUR LE BLACKHOLING

	On Path	On Path (Infraction)	Hijack		
			Type-N	Type-U	Type-O
Direct connection	✓	✓	✓	-	-
Legitimate peer	✓	✓	✓	✓	-
Direct connection	✓	✓	✓	-	✓
RPKI	✓	✓	✓	✓	-
Direct connection	✓	✓	✓	✓	✓
Legitimate peer	✓	✓	✓	✓	-
RPKI	✓	✓	✓	✓	✓
Direct connection	✓	✓	✓	✓	-
Legitimate peer	✓	✓	✓	✓	✓
RPKI	✓	✓	✓	✓	✓
Direct connection	✓	✓	✓	✓	✓
Legitimate peer	✓	✓	✓	✓	✓
RPKI	✓	✓	✓	✓	✓
BGPsec	✓	✓	✓	✓	✓
Direct connection	✓	✓	✓	✓	✓

Table 4: Protection assurée par l'addition d'une règle aux bonnes pratiques

BONNES PRATIQUES POUR LE BLACKHOLING

	On Path	On Path (Infraction)	Hijack		
			Type-N	Type-U	Type-o
Direct connection	✓	✓	✓	-	-
Legitimate peer	✓	✓	✓	✓	-
Direct connection	✓	✓	✓	-	✓
RPKI	✓	✓	✓	✓	✓
Direct connection	✓	✓	✓	✓	-
Legitimate peer	✓	✓	✓	✓	✓
RPKI	✓	✓	✓	✓	✓
Direct connection	✓	✓	✓	✓	-
Legitimate peer	✓	✓	✓	✓	✓
RPKI	✓	✓	✓	✓	✓
BGPsec	✓	✓	✓	✓	✓
Direct connection	✓	✓	✓	✓	✓
Legitimate peer	✓	✓	✓	✓	✓
RPKI	✓	✓	✓	✓	✓
BGPsec	✓	✓	✓	✓	✓
Direct connection	✓	✓	✓	✓	✓

Table 5: Protection assurée par l'addition d'une règle aux bonnes pratiques

- Bonnes pratiques additionnelles.

- Association entre les communautés et un AS.

UNE SOLUTION PASSANT PAR BGPSEC

■ Association entre les communautés et un AS.

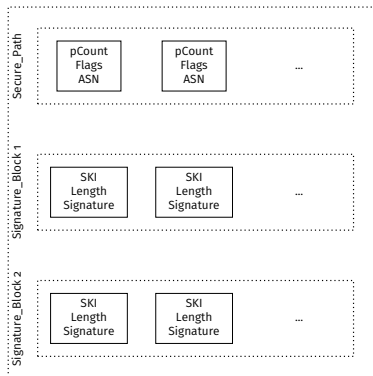


Figure 14: BGPsec_PATH attribute

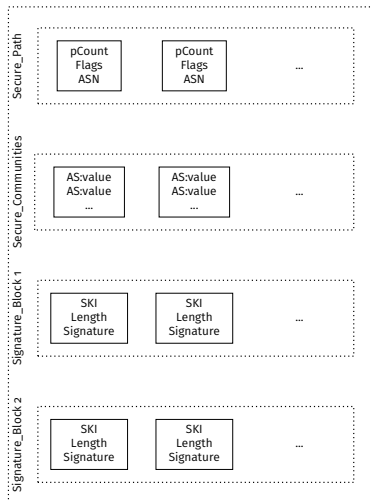


Figure 15: BGPsec_PATH_COMMUNITIES attribute

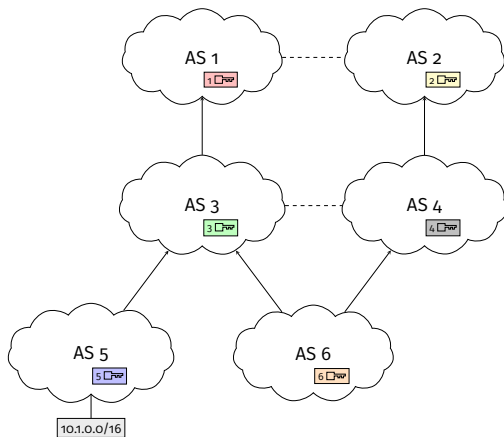


Figure 16: Propagation de messages BGPsec (modifié)

UNE SOLUTION PASSANT PAR BGPSEC

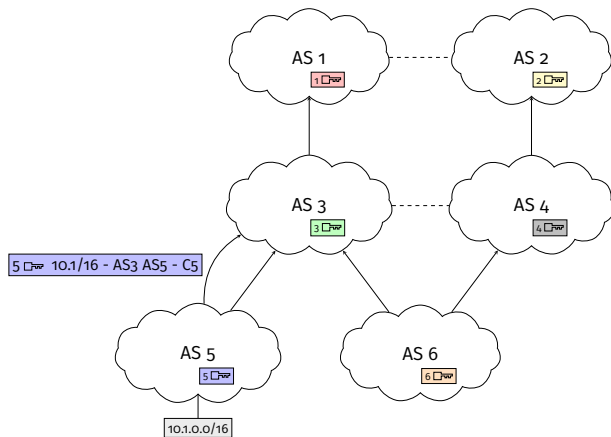


Figure 16: Propagation de messages BGPsec (modifié)

UNE SOLUTION PASSANT PAR BGPSEC

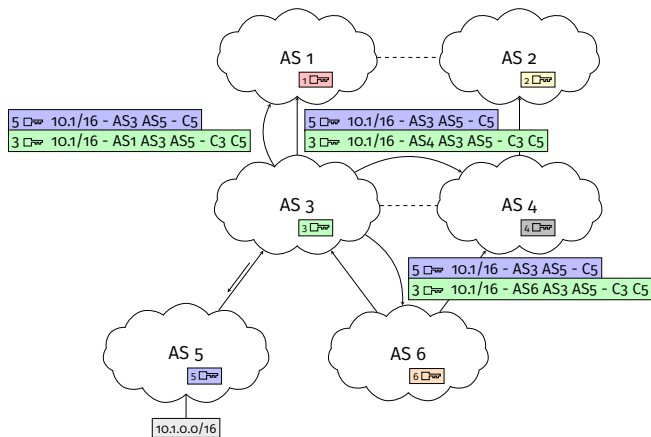


Figure 16: Propagation de messages BGPsec (modifié)

UNE SOLUTION PASSANT PAR BGPSEC

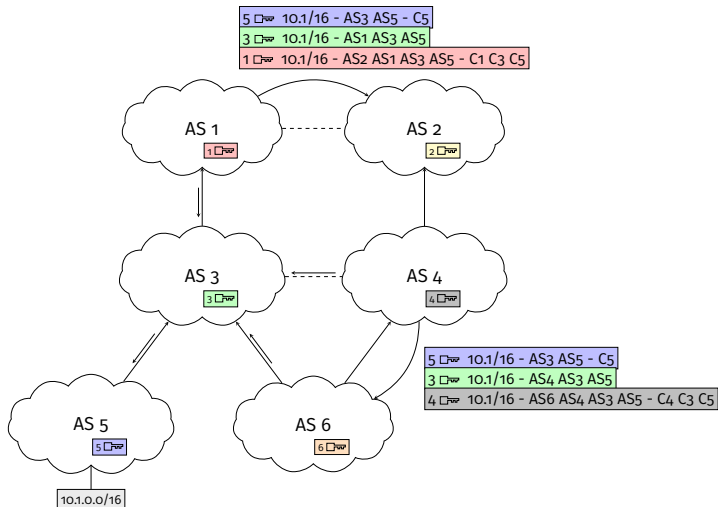


Figure 16: Propagation de messages BGPsec (modifié)

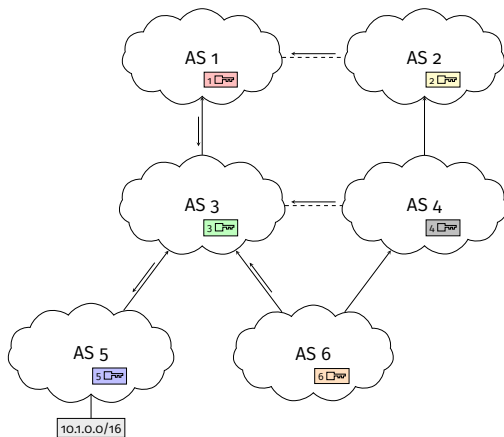


Figure 16: Propagation de messages BGPsec (modifié)

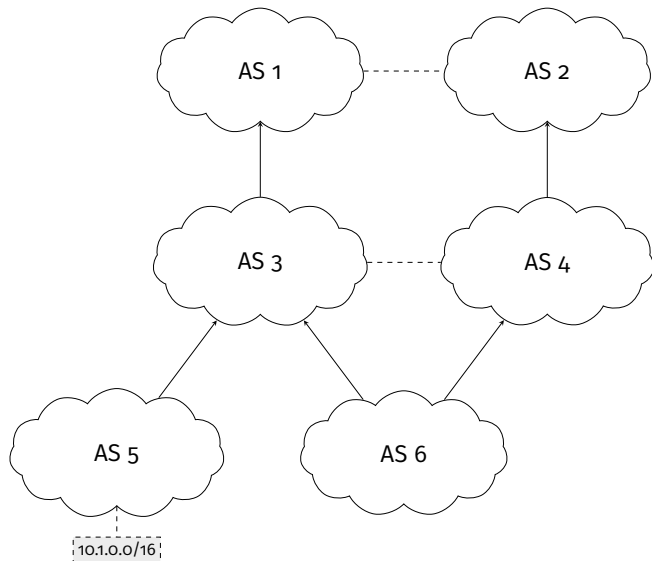


Figure 17: Topologie de test

UN OUTIL POUR DÉTECTER LES POTENTIELS ATTAQUANTS

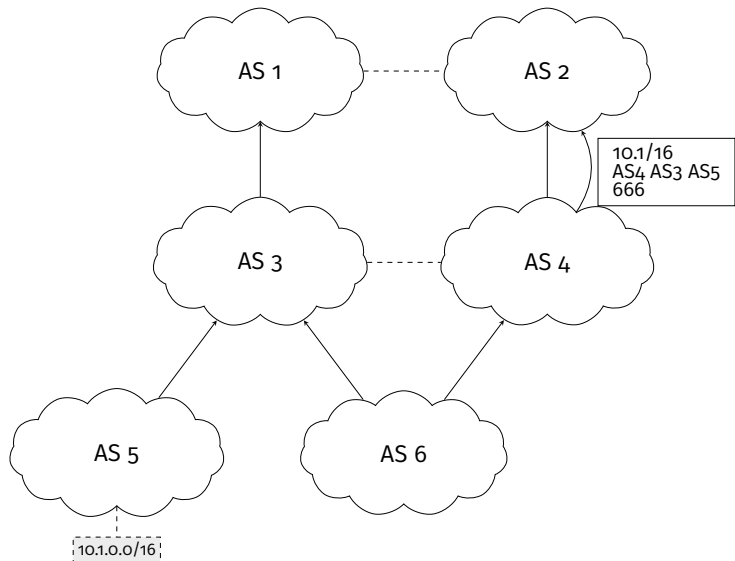


Figure 17: Topologie de test

Suppositions

- Le détecteur connaît la topologie.
- Le détecteur connaît les relations entre les AS.
- L'attaquant potentiel se trouve dans l'AS path.

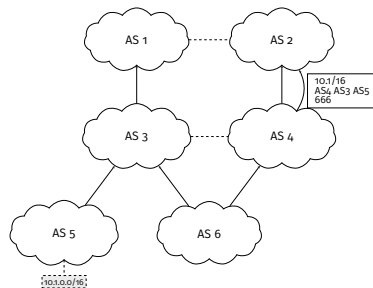


Figure 17: Topologie de test

UN OUTIL POUR DÉTECTER LES POTENTIELS ATTAQUANTS

Suppositions

- Le détecteur connaît la topologie.
- Le détecteur connaît les relations entre les AS.
- L'attaquant potentiel se trouve dans l'AS path.

Résultats

- On Path : AS3
- On Path (Infraction) : AS4
- Type-N :
- Type-o : AS5

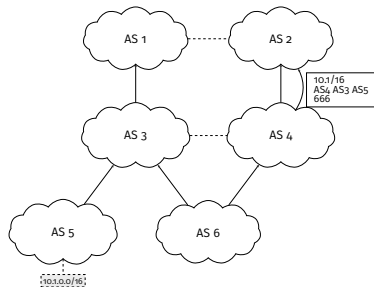


Figure 17: Topologie de test

UN OUTIL POUR DÉTECTER LES POTENTIELS ATTAQUANTS

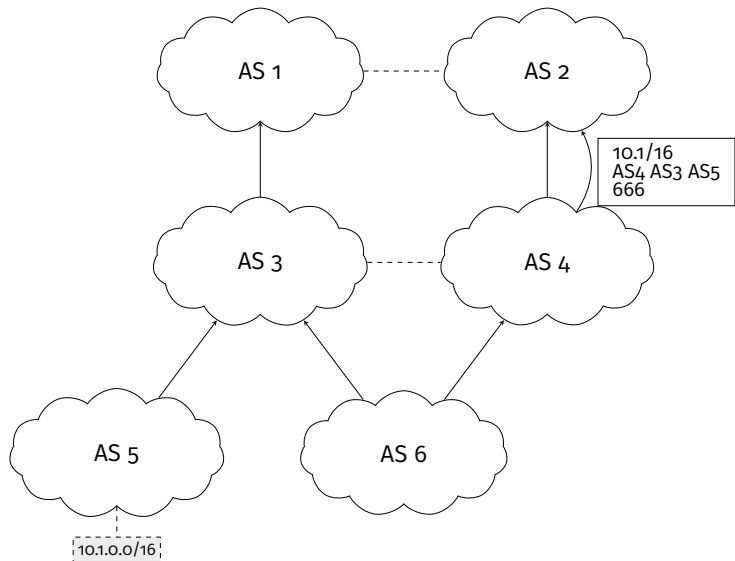


Figure 17: Topologie de test

UN OUTIL POUR DÉTECTER LES POTENTIELS ATTAQUANTS

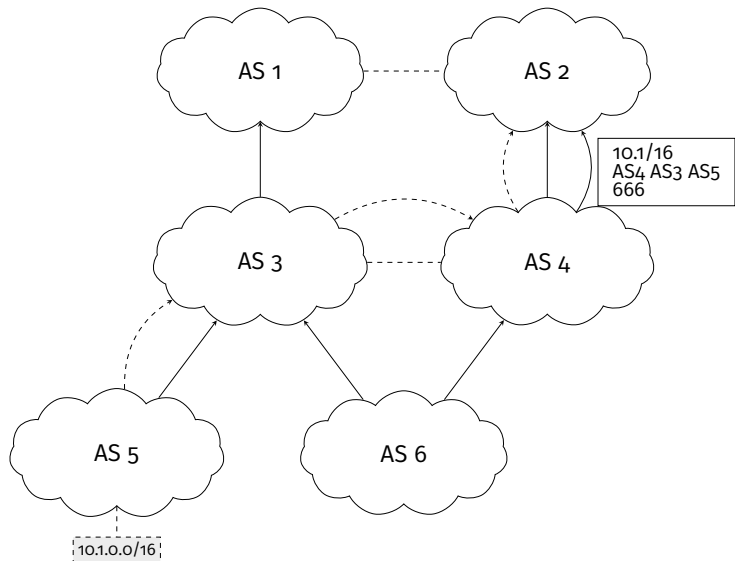


Figure 17: Topologie de test

UN OUTIL POUR DÉTECTER LES POTENTIELS ATTAQUANTS

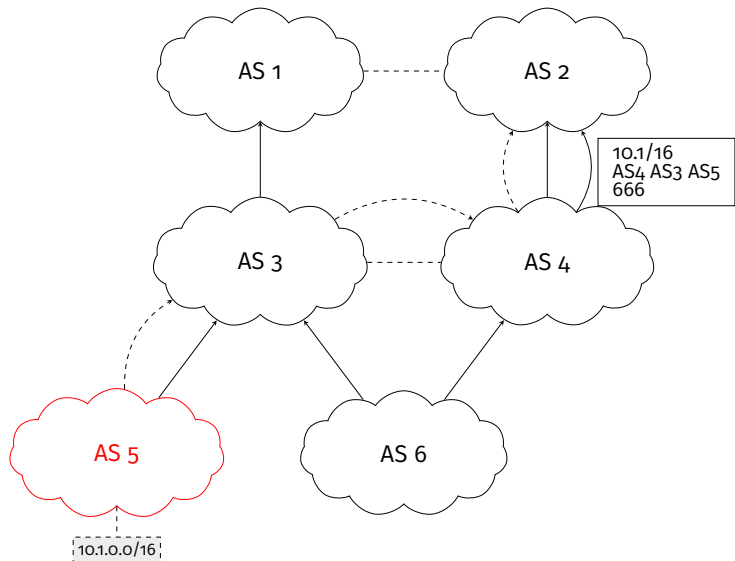


Figure 17: Topologie de test

UN OUTIL POUR DÉTECTER LES POTENTIELS ATTAQUANTS

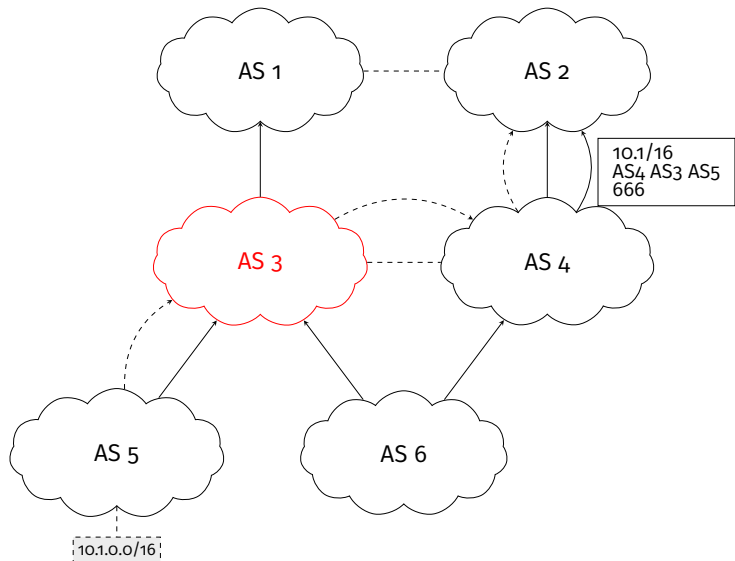


Figure 17: Topologie de test

UN OUTIL POUR DÉTECTER LES POTENTIELS ATTAQUANTS

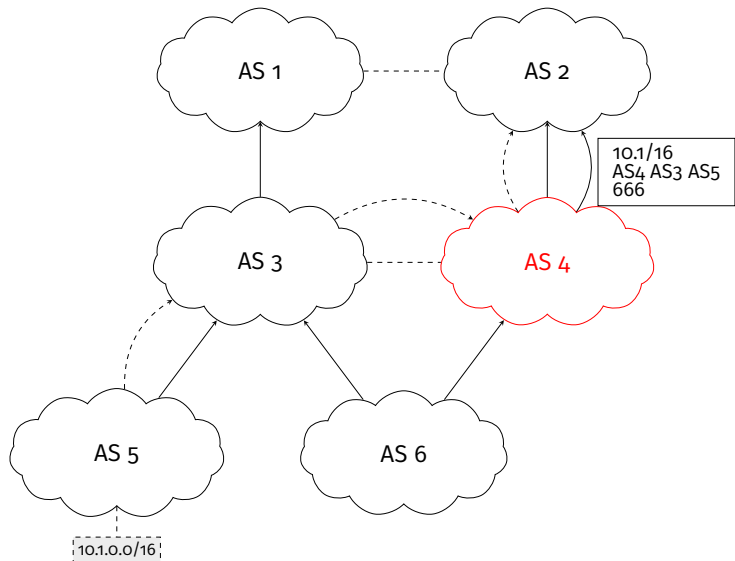


Figure 17: Topologie de test

- Taxonomies des attaques par blackholing.

- Taxonomies des attaques par blackholing.
- Des solutions passant par de bonnes pratiques.

- Taxonomies des attaques par blackholing.
- Des solutions passant par de bonnes pratiques.
- Une solution passant par une extension de BGPsec.






- Taxonomies des attaques par blackholing.
- Des solutions passant par de bonnes pratiques.
- Une solution passant par une extension de BGPsec.
- Un outil capable de détecter les attaquants potentiels.

- Tester ces contributions théoriques.

- Tester ces contributions théoriques.
- Extension du modèle d'attaque.

- Tester ces contributions théoriques.
- Extension du modèle d'attaque.
- Préciser l'extension de BGPsec.

- Tester ces contributions théoriques.
- Extension du modèle d'attaque.
- Préciser l'extension de BGPsec.
- Amélioration de l'outil.

-  Lepinski, M. and S. Kent. **An Infrastructure to Support Secure Internet Routing**. RFC 6480. RFC Editor, Feb. 2012. URL: <http://www.rfc-editor.org/rfc/rfc6480.txt>.
-  Lepinski, M. and K. Sriram. **BGPsec Protocol Specification**. RFC 8205. RFC Editor, Sept. 2017.
-  Netlab. **Insight into Global DDoS Threat Landscape**. <https://ddosmon.net/insight/>. [Online; accessed 24-August-2018]. Aug. 2018.
-  Rekhter, Y., T. Li, and S. Hares. **A Border Gateway Protocol 4 (BGP-4)**. RFC 4271. RFC Editor, Jan. 2006. URL: <http://www.rfc-editor.org/rfc/rfc4271.txt>.
-  Sermpezis, Pavlos et al. "ARTEMIS: Neutralizing BGP Hijacking within a Minute". In: **arXiv preprint arXiv:1801.01085** (2018).

- Un filtre sortant pour les annonces BGP plus spécifiques.
- Un filtre pour les annonces BGP moins spécifiques (/24 pour IPv4; /19 pour IPv6).
- Un filtre entrant sur le résultat de la validation d'origine.
- Un filtre entrant sur le résultat de la validation BGPsec.