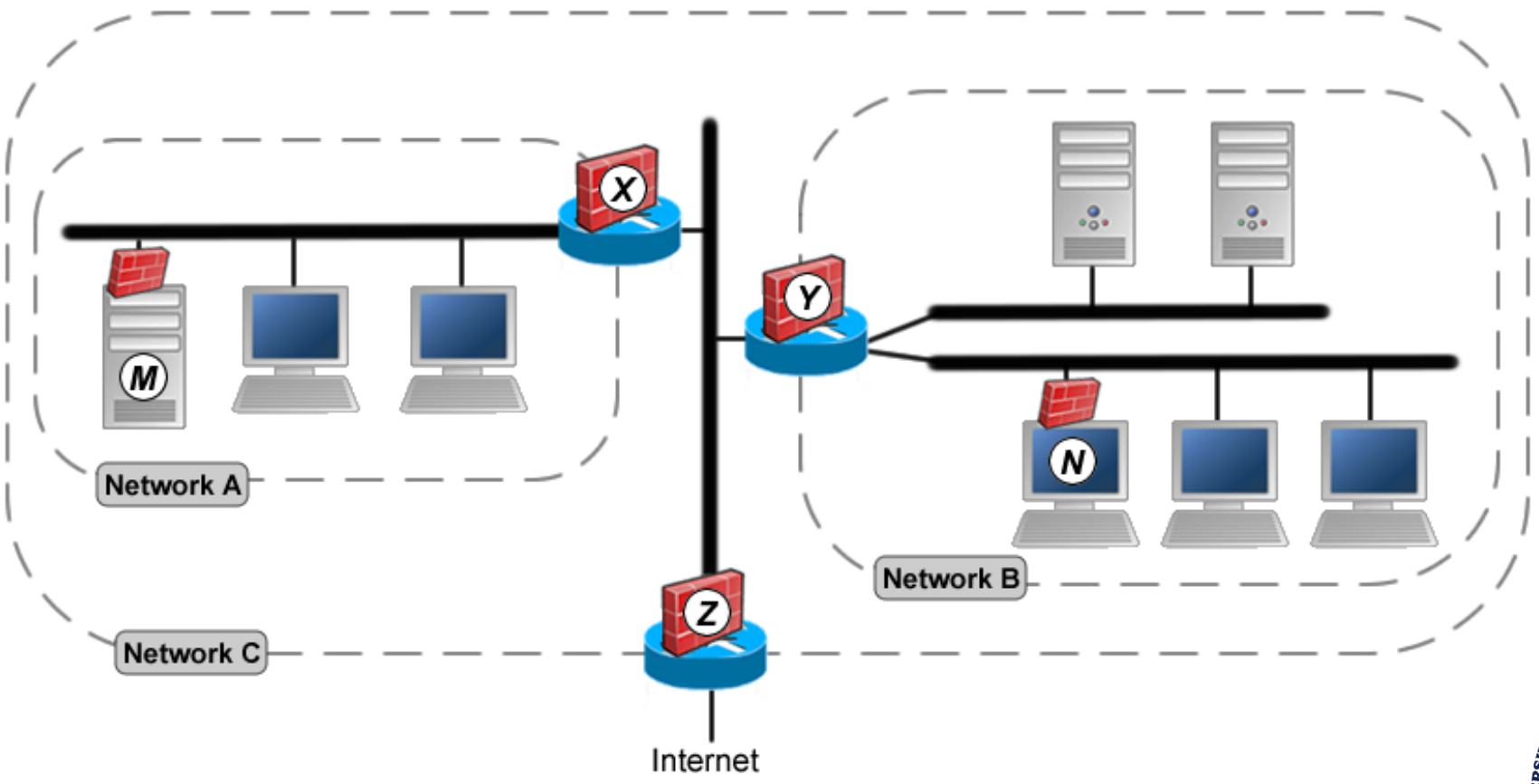
Assessment software development for distributed firewalls

Damien Leroy

Université Catholique de Louvain
Faculté des Sciences Appliquées
Département d'Ingénierie Informatique

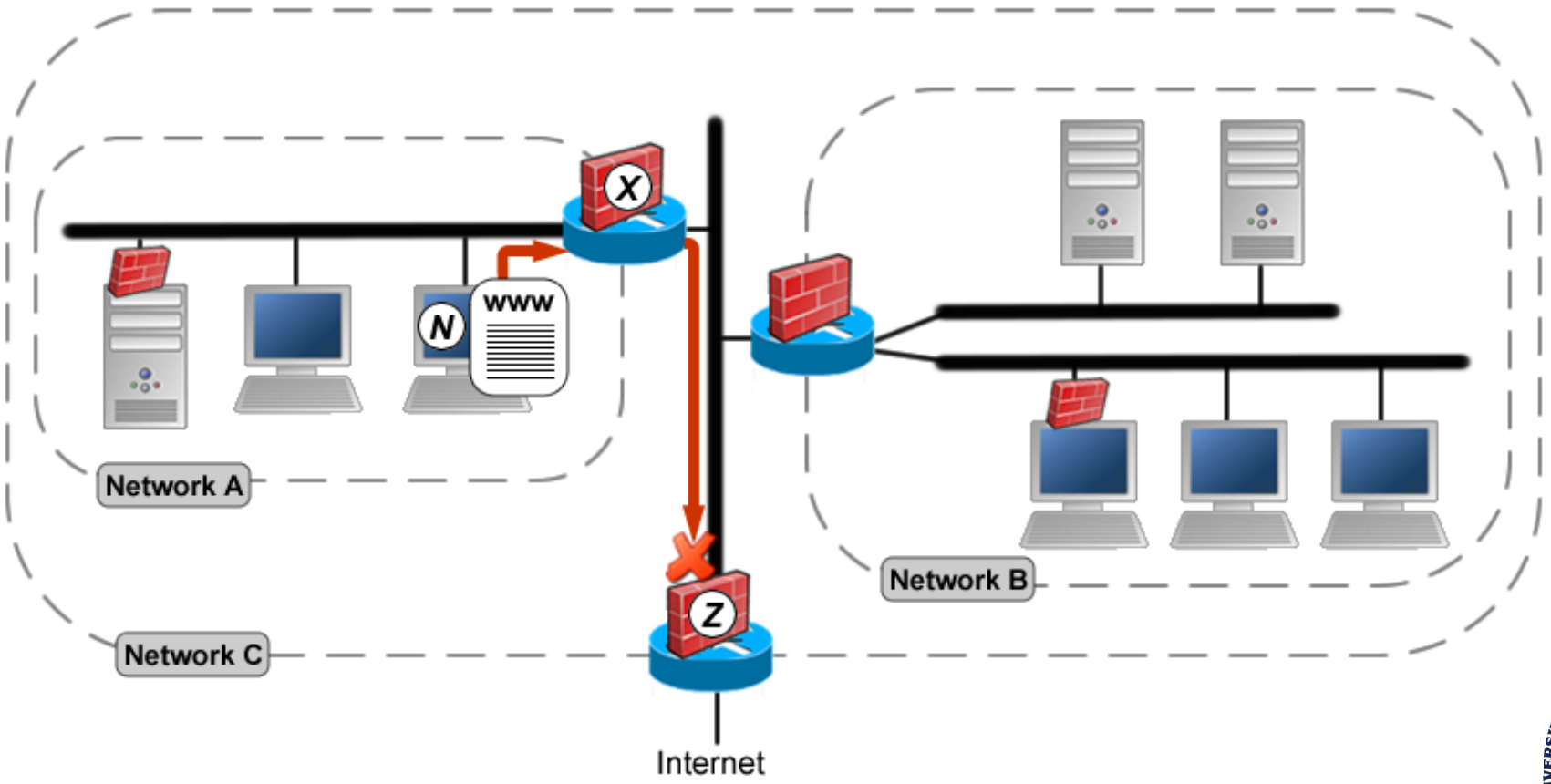
Année académique 2005-2006

Un réseau d'entreprise type



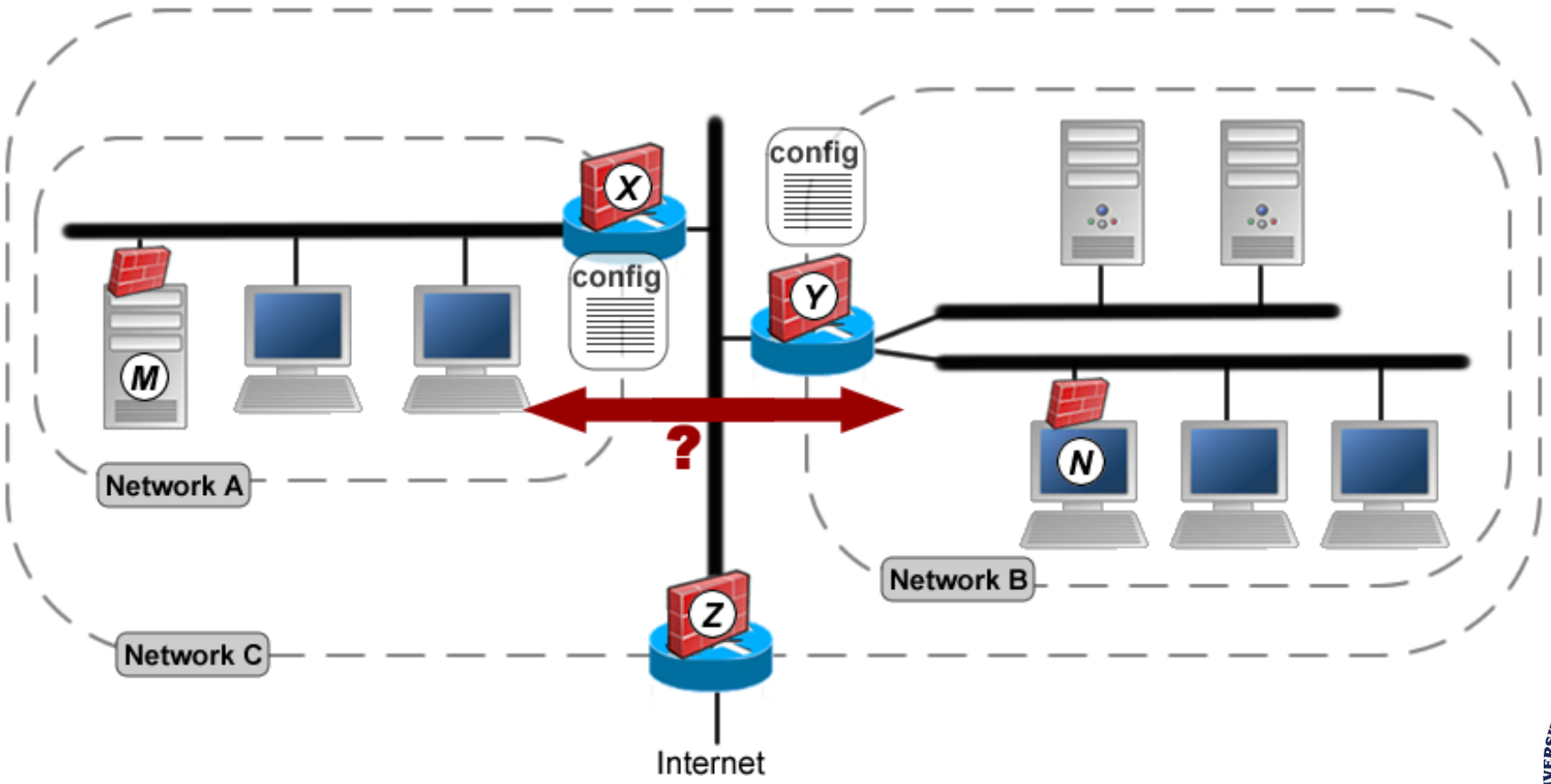
Un réseau d'entreprise type

Problème 1 : Changement de politique



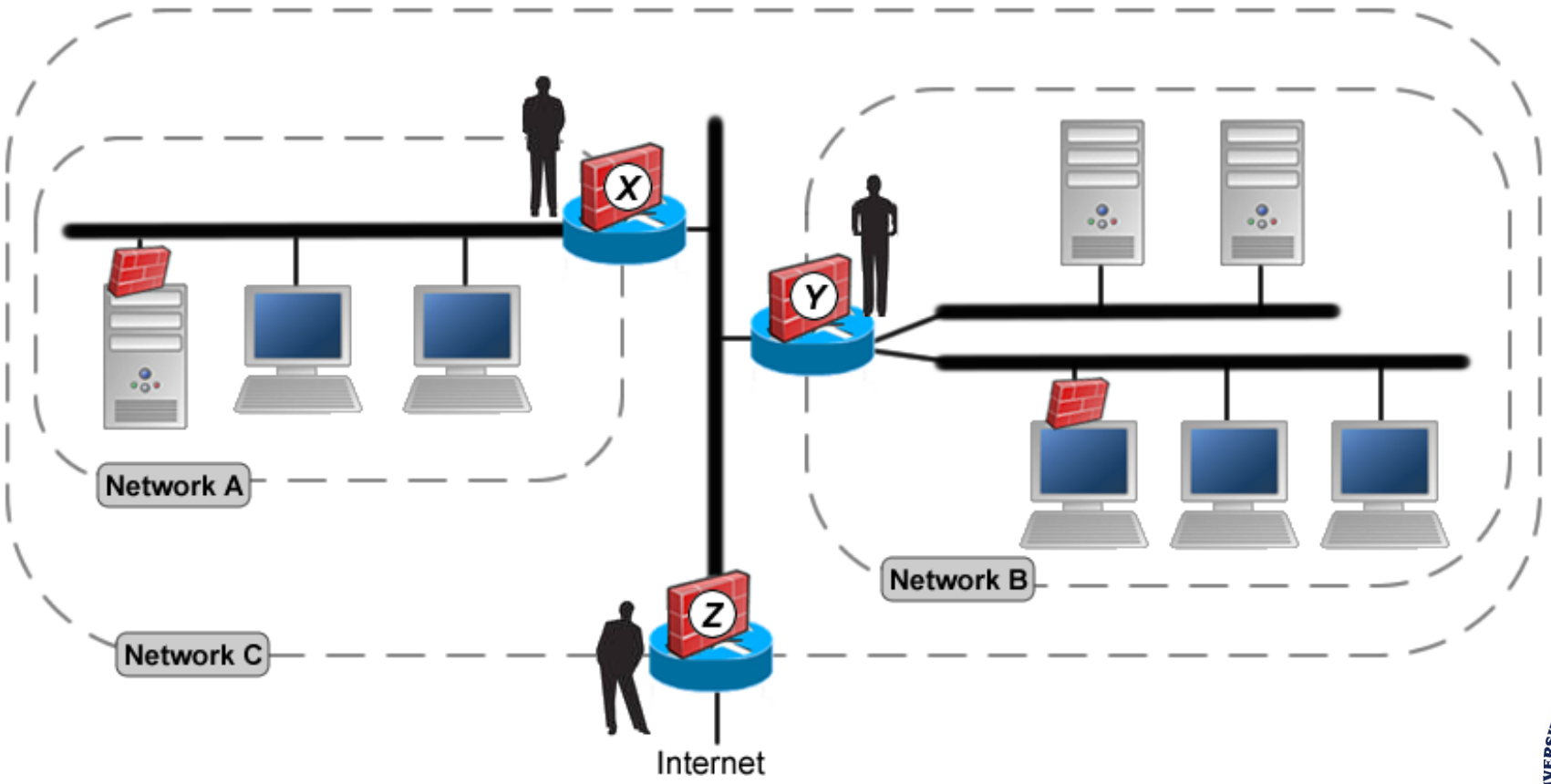
Un réseau d'entreprise type

Problème 2 : Interprétation de la politique à travers 2 firewalls



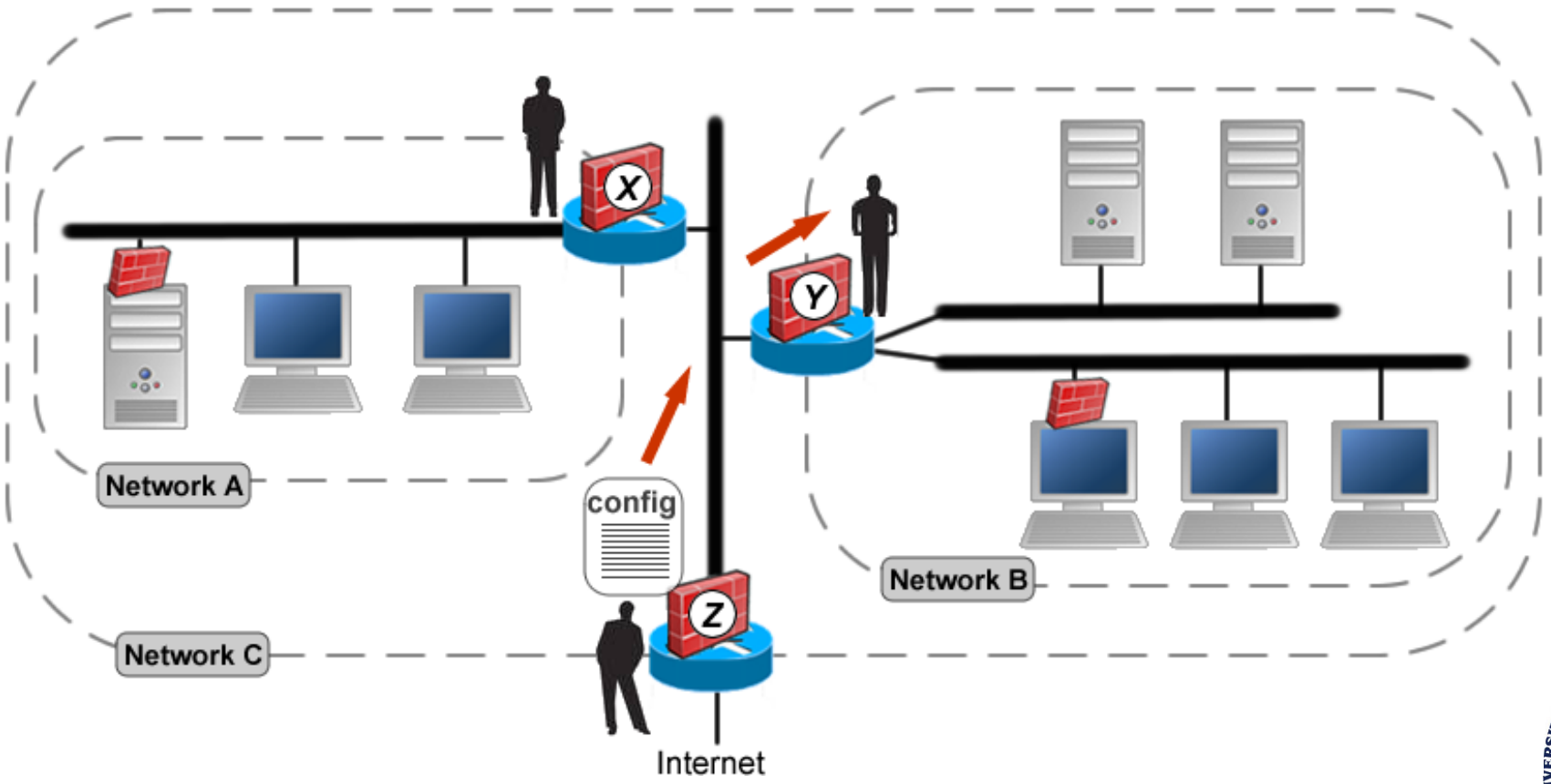
Un réseau d'entreprise type

Problème 3 : Différents administrateurs



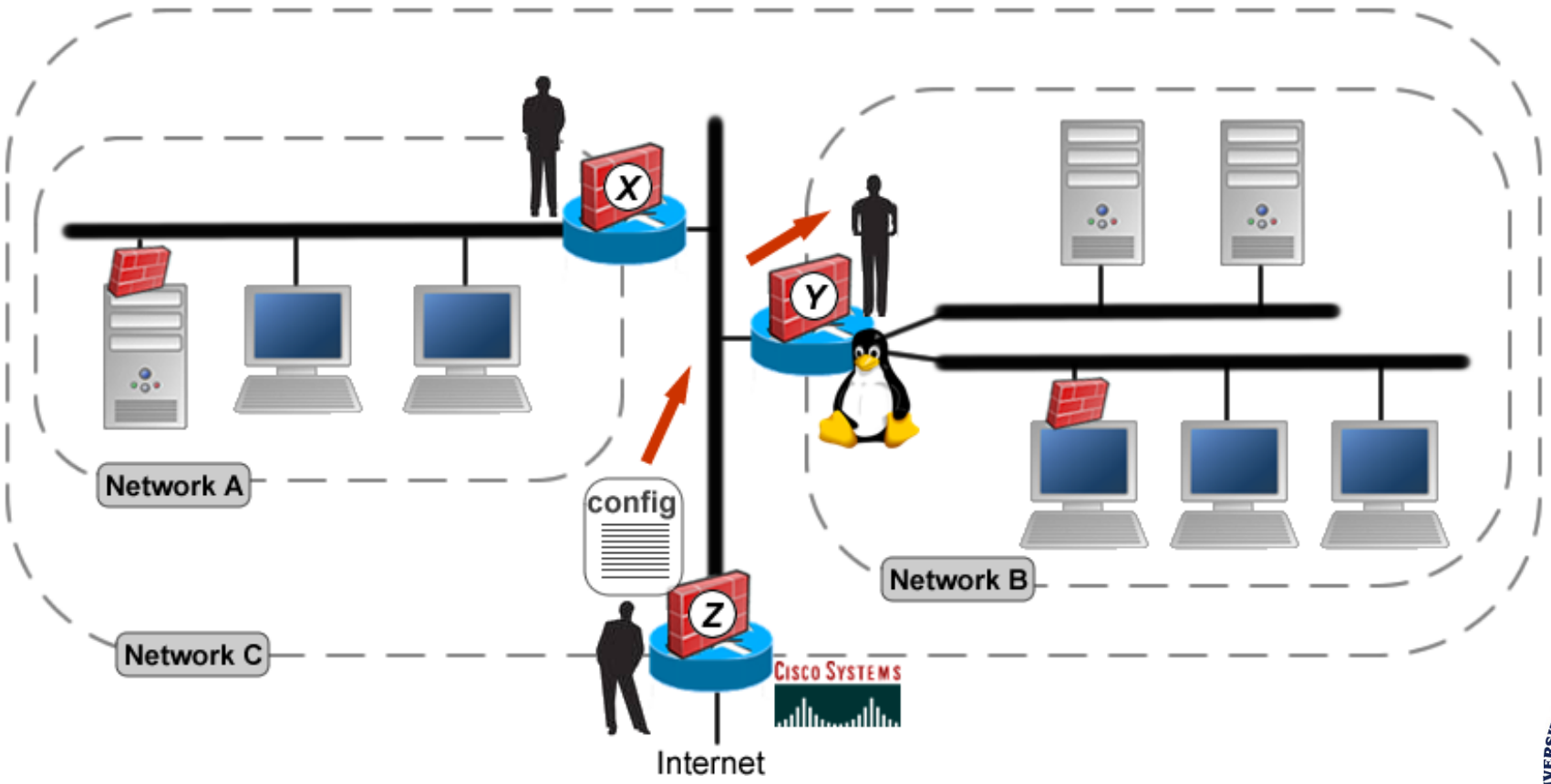
Un réseau d'entreprise type

Problème 3 : Différents administrateurs



Un réseau d'entreprise type

Problème 4 : Types de firewalls différents



Objectifs

Objectifs principaux :

- Visualisation de la politique à travers 2 firewalls
- Détection d'anomalies

Objectifs secondaires :

- Parser au moins 1 langage
- Support d'autres langages facilement
- Test sur configuration réelle

Objectifs

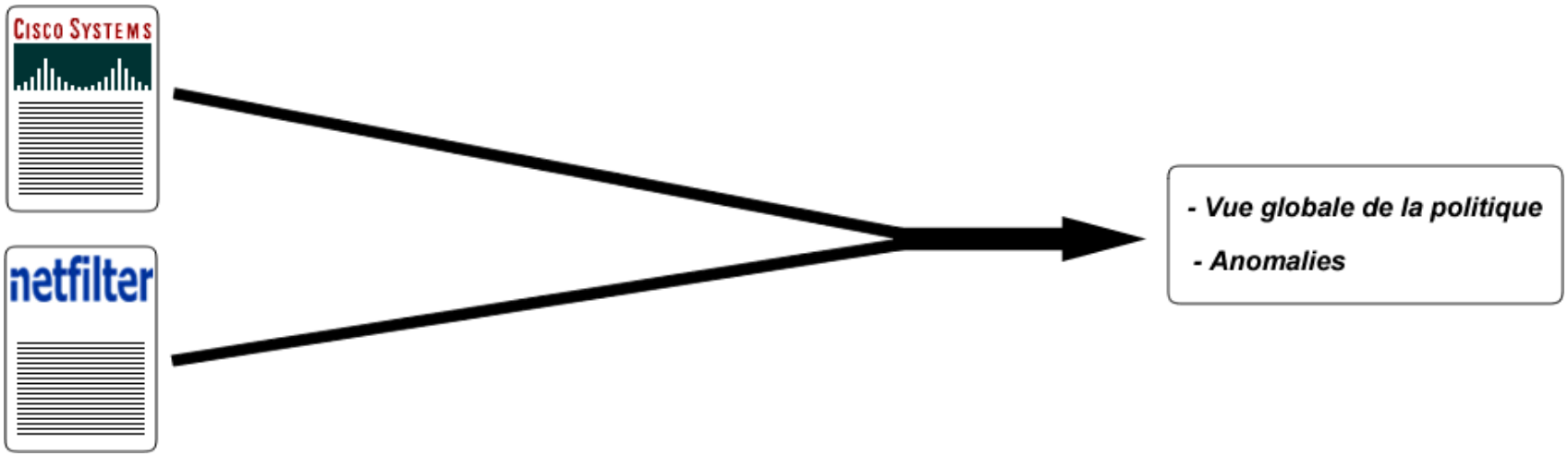
Objectifs principaux :

- Visualisation de la politique à travers 2 firewalls
- Détection d'anomalies

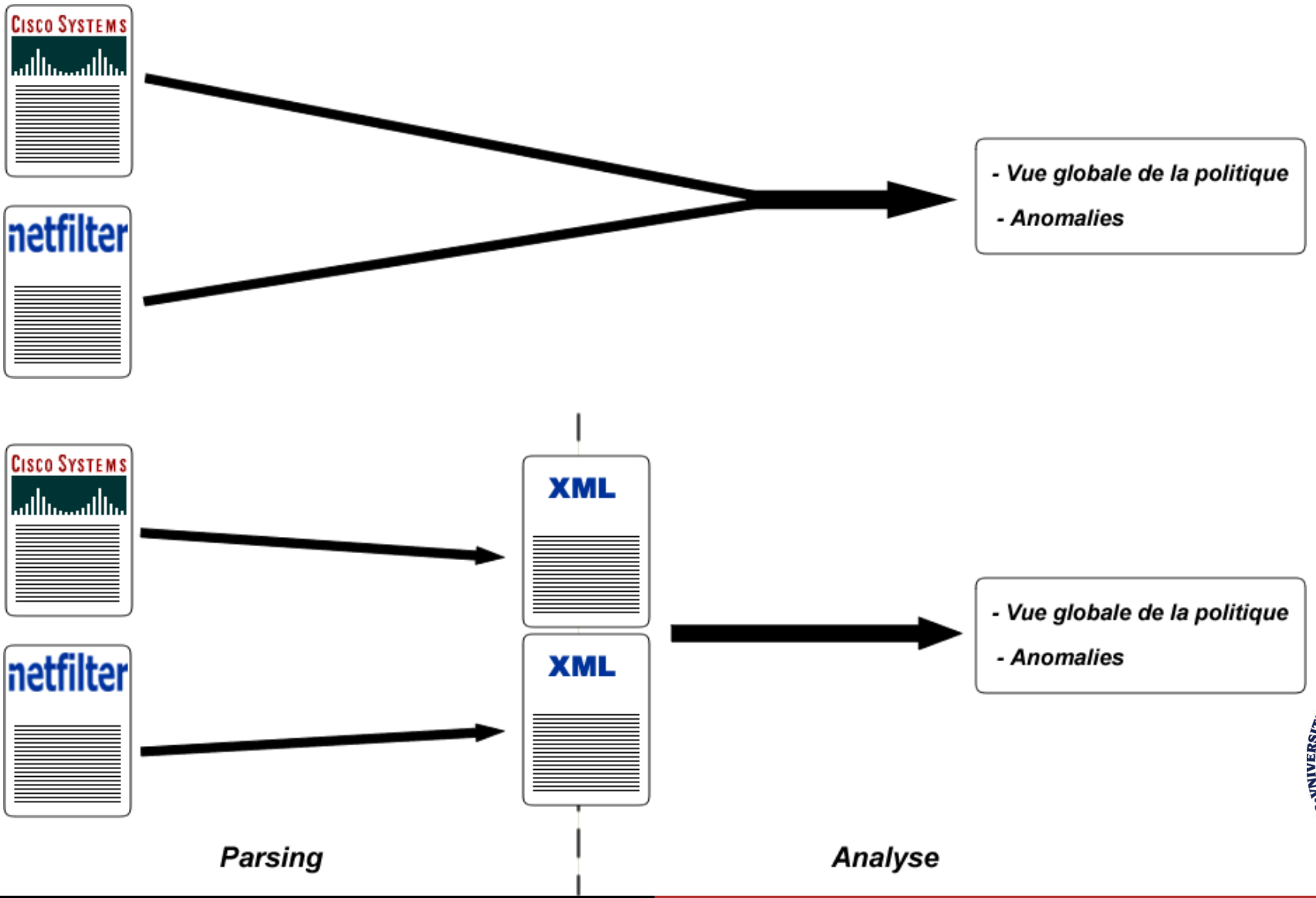
Objectifs secondaires :

- Parser au moins 1 langage
- Support d'autres langages facilement
- Test sur configuration réelle

Etapes


Cisco Systems
netfilter
- Vue globale de la politique
- Anomalies

Etapes


Cisco Systems
netfilter
- Vue globale de la politique
- Anomalies
Cisco Systems
netfilter
XML
XML
- Vue globale de la politique
- Anomalies
Parsing
Analyse

Etapes

3 grandes parties du mémoire

1. Langage pour firewalls
2. Parsing vers ce langage
3. Analyse de configuration de firewalls

Langages
Spécifications

- Suffisamment riche
- Facilement extensible

Langages
Spécifications

- Suffisamment riche
- Facilement extensible

Langages
Exemple

```
<?xml version="1.0" encoding="UTF-8"?>
<firewall srclang="Iptables (iptables-save)">
  <filtertable>
    <frule target="DROP">
      <protocol inverted="false">tcp</protocol>
      <interfacein inverted="true">eth0</interfacein>
      <ipv4>
        <src inverted="false">
          <ip>1.2.3.4</ip>
        </src>
        <dst inverted="false"> ... </dst>
      </ipv4>
    </frule>
    <frule target="ACCEPT"> ... </frule>
    [...]
  </filtertable>
  <interface>...</interface>
</firewall>
```

Langages
Exemple

```
<?xml version="1.0" encoding="UTF-8"?>
<firewall srclang="Iptables (iptables-save)">
  <filtertable>
    <frule target="DROP">
      <protocol inverted="false">tcp</protocol>
      <interfacein inverted="true">eth0</interfacein>
      <ipv4>
        <src inverted="false">
          <ip>1.2.3.4</ip>
        </src>
        <dst inverted="false"> ... </dst>
      </ipv4>
    </frule>
    <frule target="ACCEPT"> ... </frule>
    [...]
  </filtertable>
  <interface>...</interface>
</firewall>
```

Langages
Exemple

```
<?xml version="1.0" encoding="UTF-8"?>
<firewall srclang="Iptables (iptables-save)">
  <filtertable>
    <frule target="DROP">
      <protocol inverted="false">tcp</protocol>
      <interfacein inverted="true">eth0</interfacein>
      <ipv4>
        <src inverted="false">
          <ip>1.2.3.4</ip>
        </src>
        <dst inverted="false"> ... </dst>
      </ipv4>
    </frule>
    <frule target="ACCEPT"> ... </frule>
    [...]
  </filtertable>
  <interface>...</interface>
</firewall>
```

Langages
Exemple

```
<?xml version="1.0" encoding="UTF-8"?>
<firewall srclang="Iptables (iptables-save)">
  <filtertable>
    <frule target="DROP">
      <protocol inverted="false">tcp</protocol>
      <interfacein inverted="true">eth0</interfacein>
      <ipv4>
        <src inverted="false">
          <ip>1.2.3.4</ip>
        </src>
        <dst inverted="false"> ... </dst>
      </ipv4>
    </frule>
    <frule target="ACCEPT"> ... </frule>
    [...]
  </filtertable>
  <interface>...</interface>
</firewall>
```

Langages
Exemple

```
<?xml version="1.0" encoding="UTF-8"?>
<firewall srclang="Iptables (iptables-save)">
  <filtertable>
    <frule target="DROP">
      <protocol inverted="false">tcp</protocol>
      <interfacein inverted="true">eth0</interfacein>
      <ipv4>
        <src inverted="false">
          <ip>1.2.3.4</ip>
        </src>
        <dst inverted="false"> ... </dst>
      </ipv4>
    </frule>
    <frule target="ACCEPT"> ... </frule>
    [...]
  </filtertable>
  <interface>...</interface>
</firewall>
```

Langages
Exemple

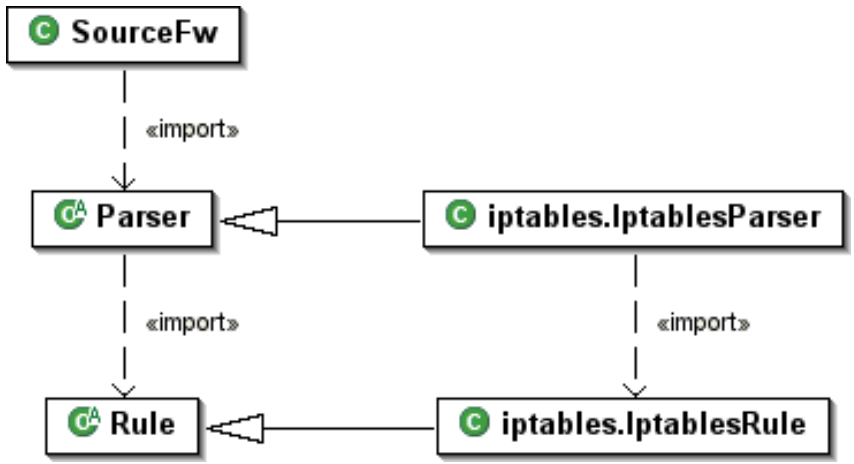
```
<?xml version="1.0" encoding="UTF-8"?>
<firewall srclang="Iptables (iptables-save)">
  <filtertable>
    <frule target="DROP">
      <protocol inverted="false">tcp</protocol>
      <interfacein inverted="true">eth0</interfacein>
      <ipv4>
        <src inverted="false">
          <ip>1.2.3.4</ip>
        </src>
        <dst inverted="false"> ... </dst>
      </ipv4>
    </frule>
    <frule target="ACCEPT"> ... </frule>
    [...]
  </filtertable>
  <interface>...</interface>
</firewall>
```

Langages
Exemple

```
<?xml version="1.0" encoding="UTF-8"?>
<firewall srclang="Iptables (iptables-save)">
  <filtertable>
    <frule target="DROP">
      <protocol inverted="false">tcp</protocol>
      <interfacein inverted="true">eth0</interfacein>
      <ipv4>
        <src inverted="false">
          <ip>1.2.3.4</ip>
        </src>
        <dst inverted="false"> ... </dst>
      </ipv4>
    </frule>
    <frule target="ACCEPT"> ... </frule>
    [...]
  </filtertable>
  <interface>...</interface>
</firewall>
```

Parser

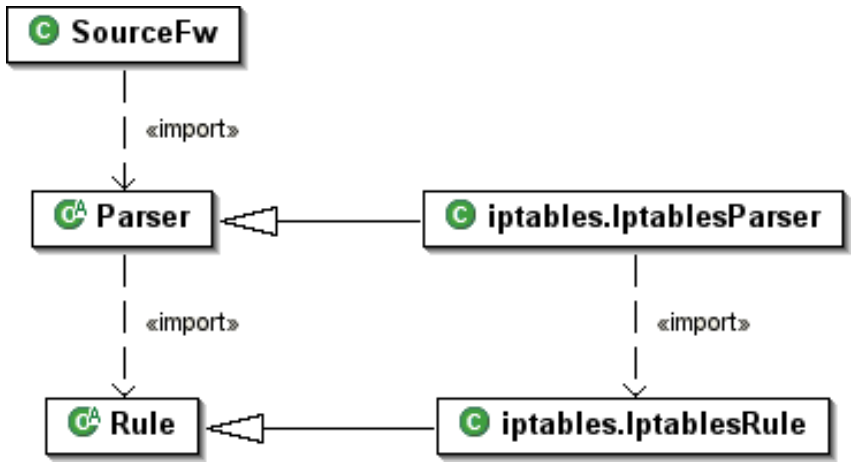
- Classes générales, étendues pour méthodes spécifiques aux langages



- Implémenté pour *Netfilter/iptables*

Parser

- Classes générales, étendues pour méthodes spécifiques aux langages



- Implémenté pour *Netfilter/iptables*

Parser

Chaînes *iptables*

```
fwd : prot=TCP & dst_port=0-1024 & src_ip=1.0.1.0/24 => chain1
chain1 : src_port=30 & prot=ESP => chain2
chain1 : dst_port=80 => chain2
chain1 : => DROP
chain2 : dst_ip=1.2.3.4 & src_ip=1.0.0.0/8 => ACCEPT
chain2 : dst_ip=4.0.0.0/0 & !fragment => ACCEPT
```

Parser

Chaînes *iptables*

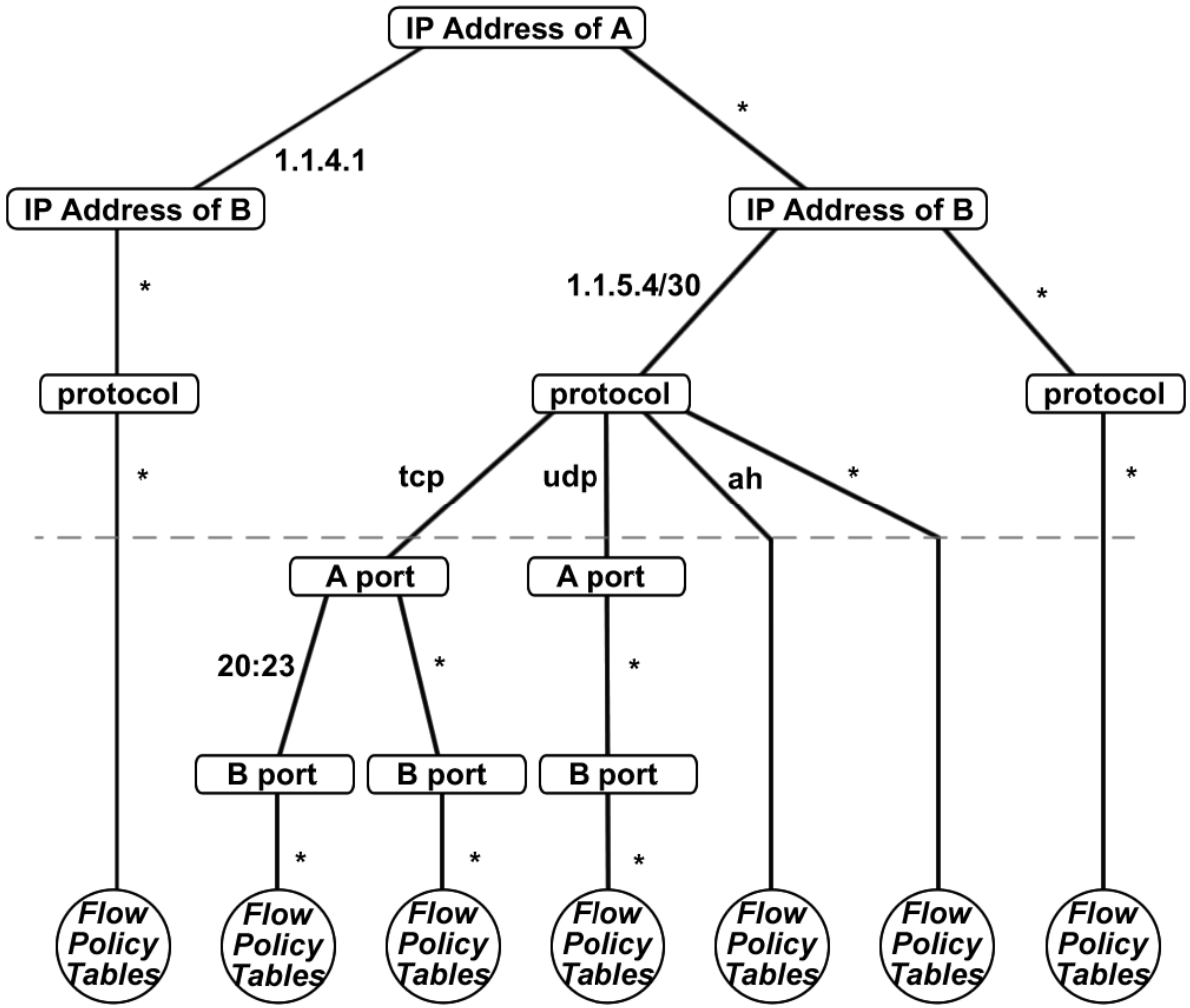
```
fwd : prot=TCP & dst_port=0-1024 & src_ip=1.0.1.0/24 => chain1
chain1 : src_port=30 & prot=ESP => chain2
chain1 : dst_port=80 => chain2
chain1 : => DROP
chain2 : dst_ip=1.2.3.4 & src_ip=1.0.0.0/8 => ACCEPT
chain2 : dst_ip=4.0.0.0/0 & !fragment => ACCEPT
```

$\longrightarrow$ Parfois difficile à interpréter

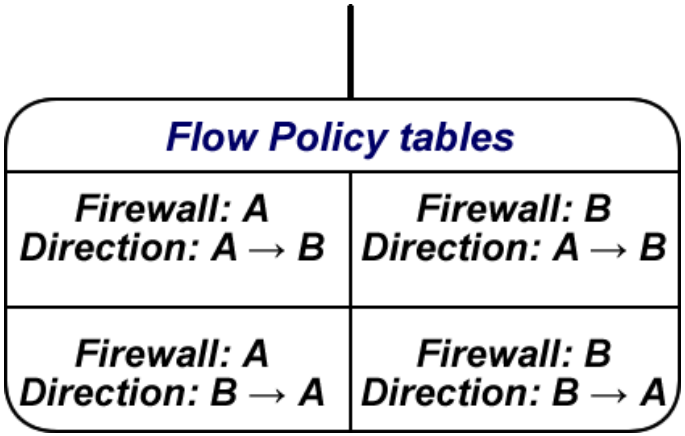
Analyse

- Visualisation de la politique générale : policy tree
- Détection d'anomalies

Analyse
Policy tree



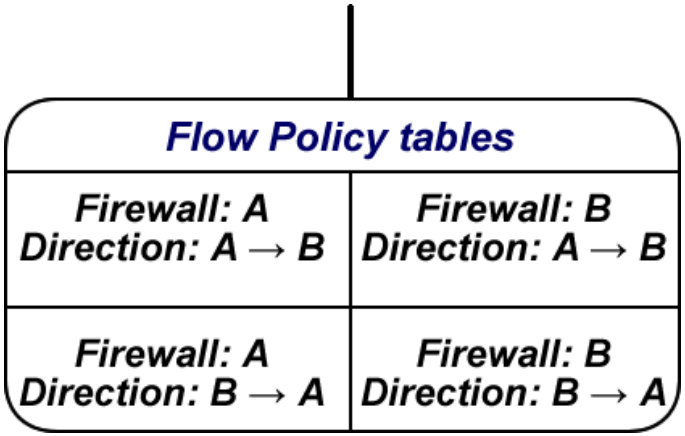
Analyse
Policy tree



La politique de chaque table :

- ACCEPT
- DROP
- ESTABLISHED

Analyse
Policy tree

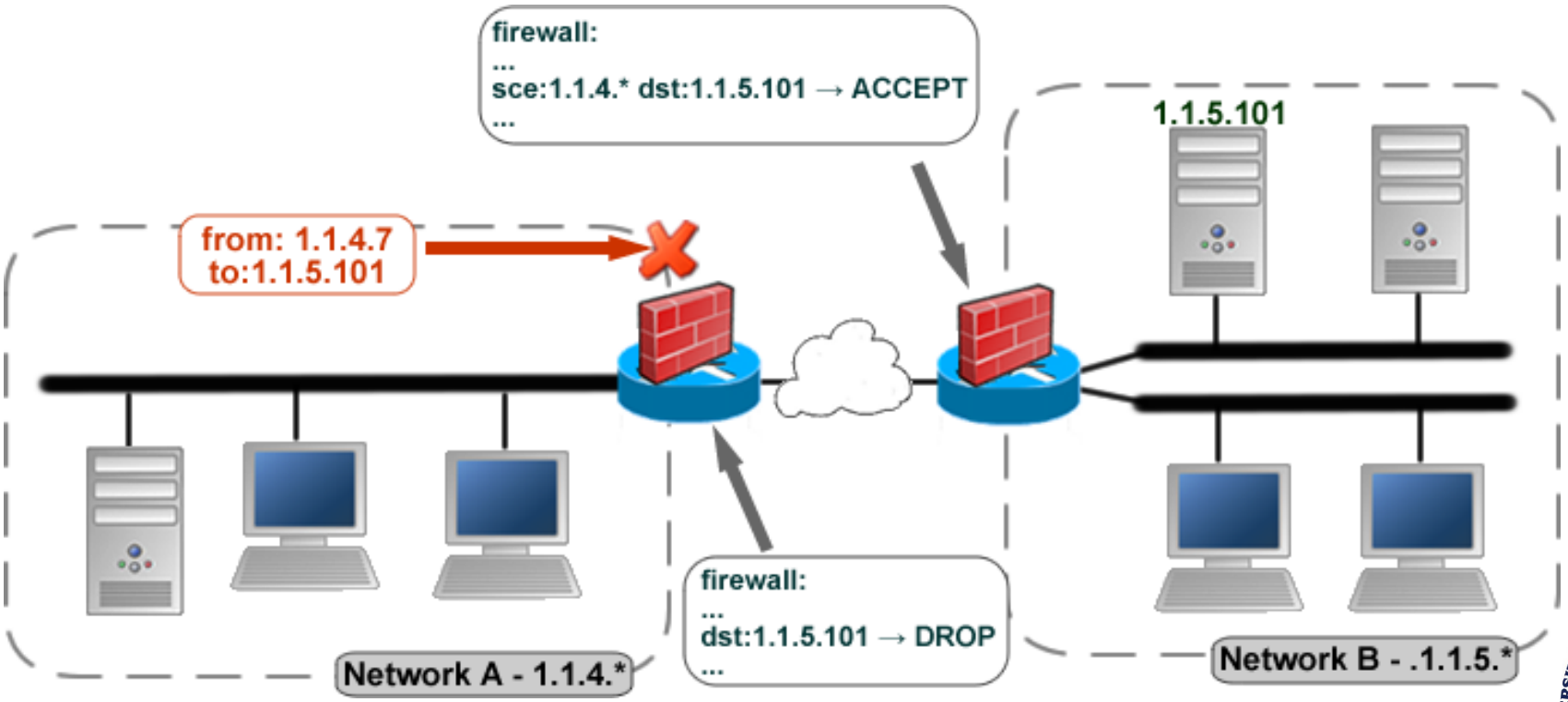


La politique de chaque table :

- ACCEPT
- DROP
- ESTABLISHED

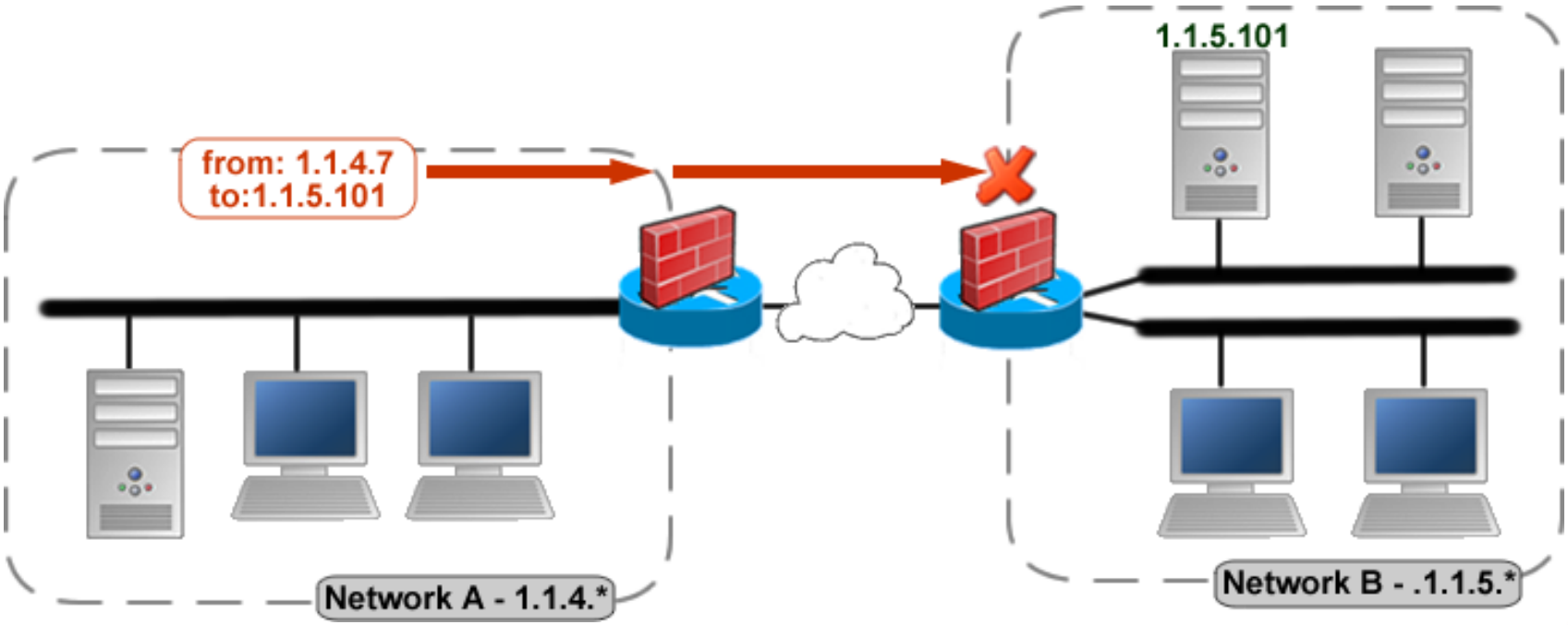
Analyse
Anomalies

1. Upstream blocked anomaly



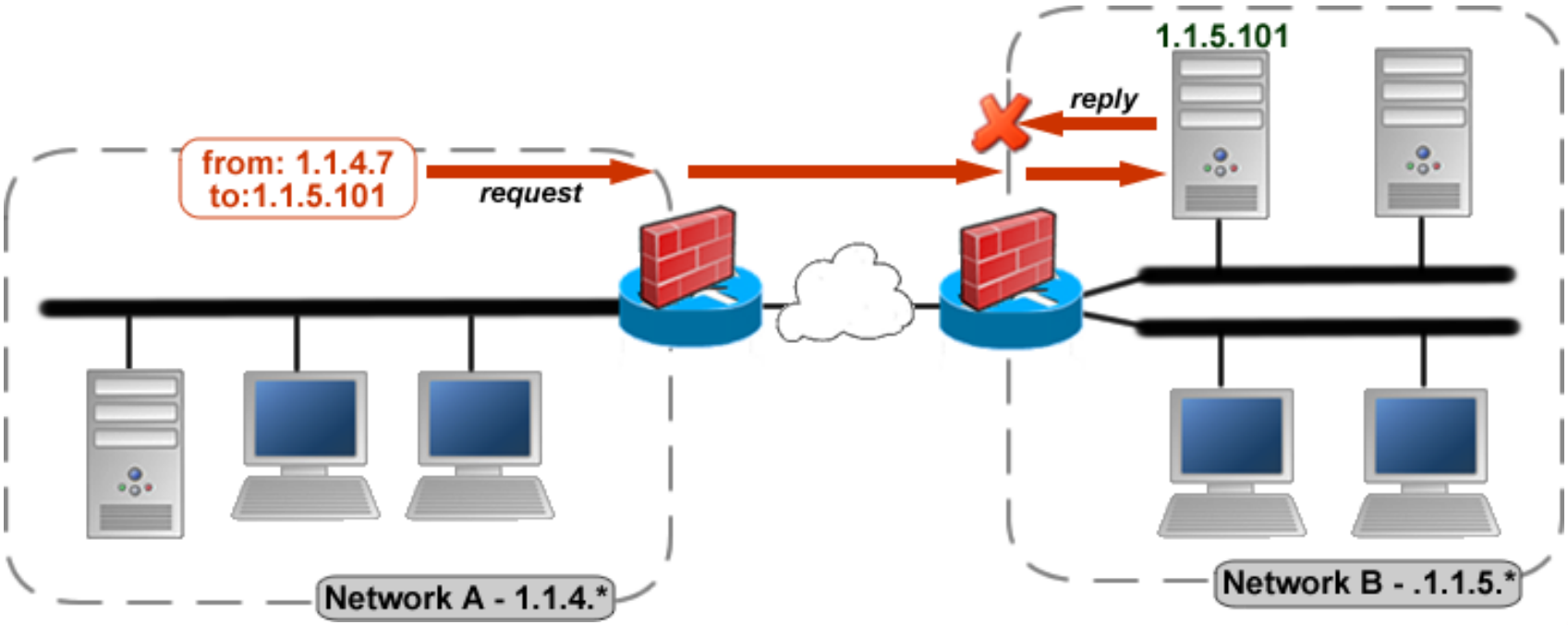
Analyse
Anomalies

2. Downstream blocked anomaly



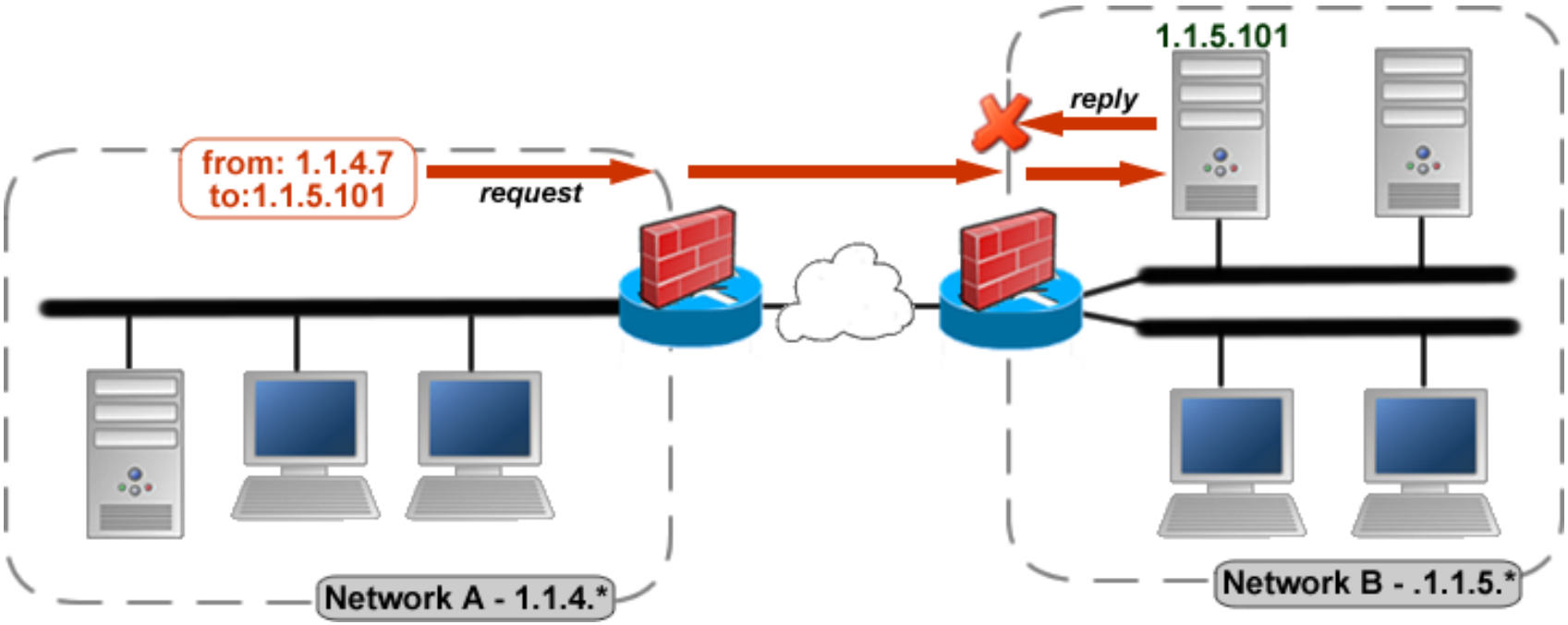
Analyse
Anomalies

3. No reply anomaly



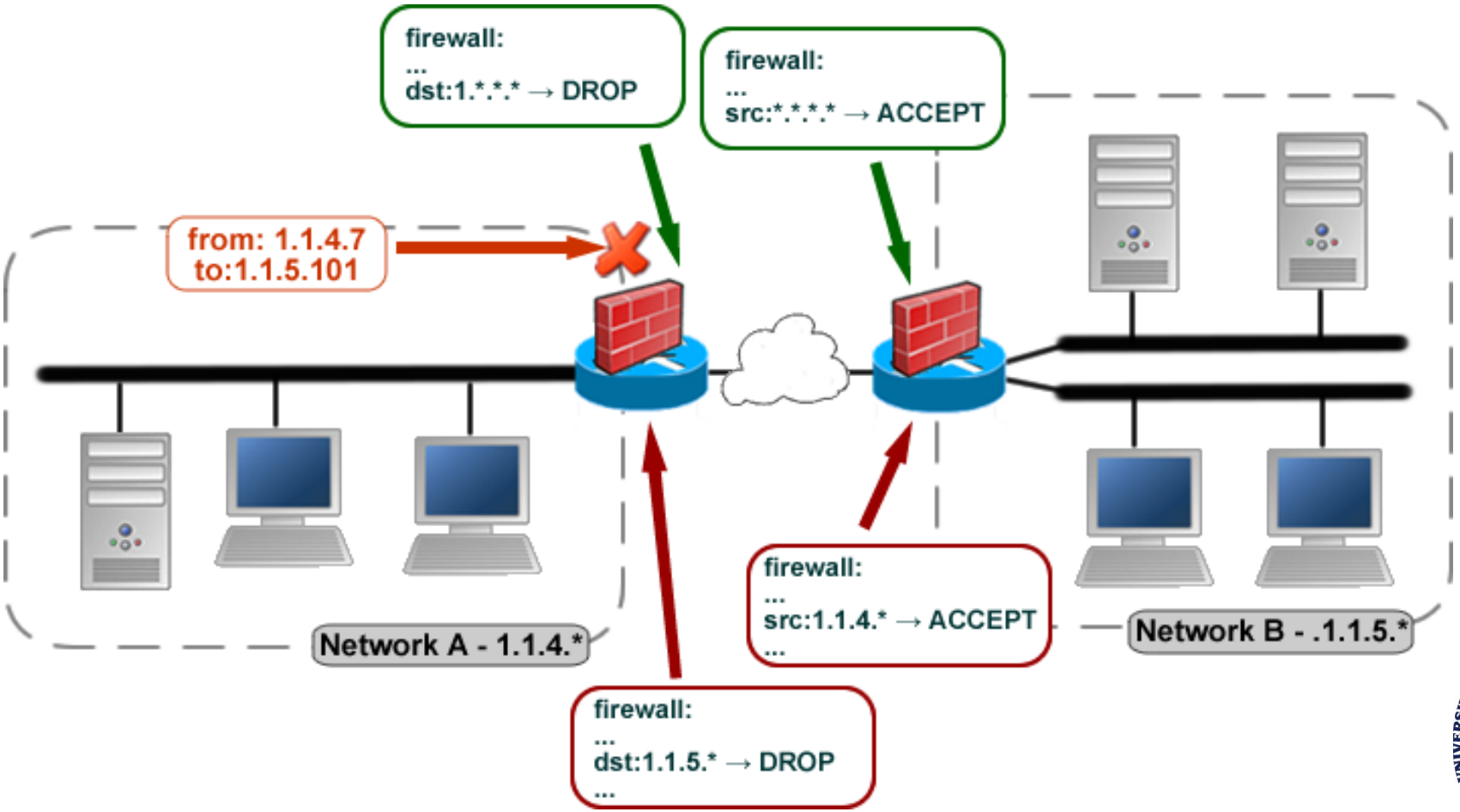
Analyse
Anomalies

3. No reply anomaly



4. Useless established anomaly

Analyse
Anomalies plus significatives



Principaux problèmes rencontrés

- Suppression des chaînes de *Netfilter/iptables*
- Construction du policy tree
- Place en mémoire du policy tree

Limitations

- NAT non supporté
- Pertinance des anomalies détectées pour l'instant
- Uniquement configuration *Netfilter/iptables* analysées

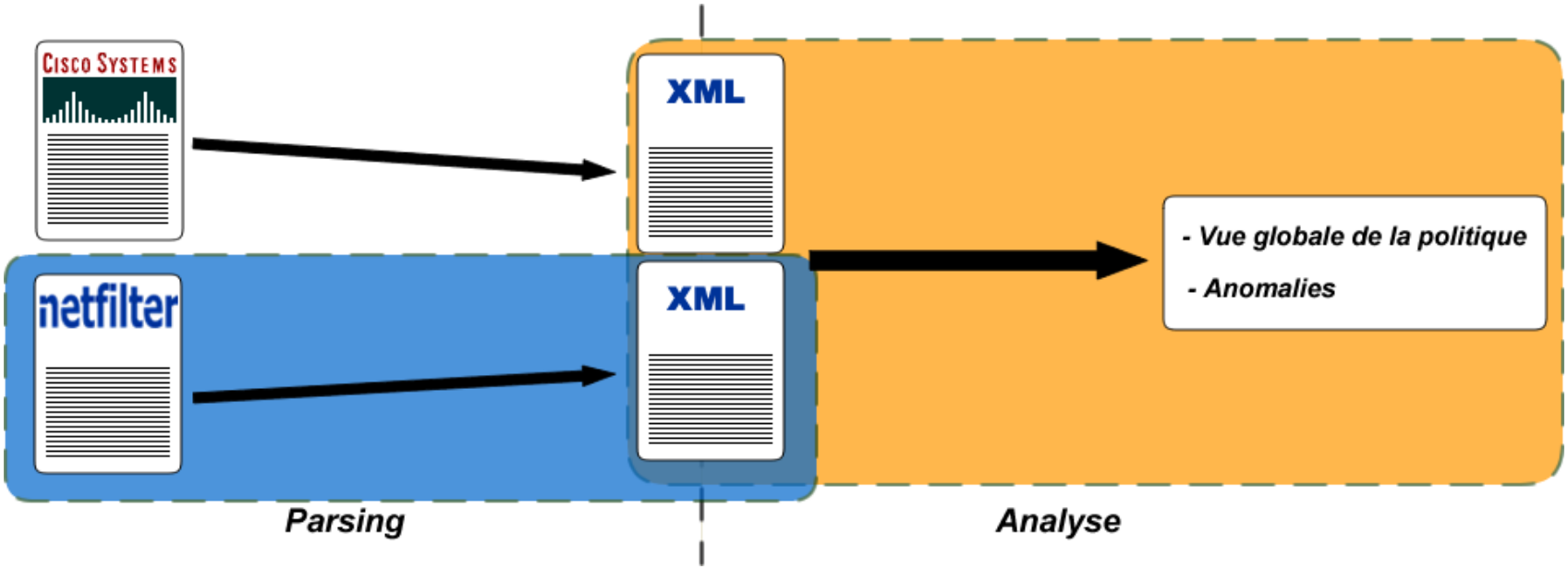
Limitations

- NAT non supporté
- Pertinance des anomalies détectées pour l'instant
- Uniquement configuration *Netfilter/iptables* analysées

Limitations

- NAT non supporté
- Pertinance des anomalies détectées pour l'instant
- Uniquement configuration *Netfilter/iptables* analysées

Forces du travail



Quelques pistes à poursuivre

- D'autres parsers
- Parser dans d'autres contextes
- Parser et policy tree pour d'autres analyses de firewalls
- Détection d'autres anomalies ou de plus pertinantes

Quelques pistes à poursuivre

- D'autres parsers
- Parser dans d'autres contextes
- Parser et policy tree pour d'autres analyses de firewalls
- Détection d'autres anomalies ou de plus pertinantes

Quelques pistes à poursuivre

- D'autres parsers
- Parser dans d'autres contextes
- Parser et policy tree pour d'autres analyses de firewalls
- Détection d'autres anomalies ou de plus pertinantes

Quelques pistes à poursuivre

- D'autres parsers
- Parser dans d'autres contextes
- Parser et policy tree pour d'autres analyses de firewalls
- Détection d'autres anomalies ou de plus pertinantes

Conclusion


UNIVERSITAS CATHOLICA LOVANIENSIS
1425
SEDES SAPIENTIAE

Merci de votre attention

Des questions ?