

ALOHA LOAD BALANCER CONFIGURATION POUR TREND INTERSCAN WEB SECURITY

« APPNOTES » #0043 — TREND INTERSCAN WEB SECURITY

Cette note applicative a pour vocation de vous aider à répartir la charge sur plusieurs passerelles anti-malwares et de filtrages Trend InterScan Web Security grâce à la solution ALOHA Load Balancer.

CONTRAINTE

Les passerelles Trend InterScan Web Security devront être configurées en mode « Forward proxy » tel qu'indiqué ci-dessous.

The screenshot shows the configuration page for the Trend Micro InterScan Web Security Virtual Appliance. The left sidebar contains a navigation menu with categories like Summary, HTTP, FTP, Reports, Logs, Updates, Notifications, and Administration. The main content area is titled 'Deployment Mode' and has two tabs: 'Deployment Mode' (active) and 'User Identification'. Under 'Deployment Mode', there are several options: 'Transparent bridge' (disabled), 'Forward proxy' (selected), 'Enable upstream proxy (dependent mode)' (disabled), 'Enable guest account' (disabled), and 'Enable transparency' (disabled). Under 'Enable transparency', there are two radio buttons: 'Use simple transparency' (selected) and 'Use Web Cache Coordination Protocol (WCCP)'. The 'WCCP Forwarding Method' section has two radio buttons: 'GRE (Generic Routing Encapsulation)' (selected) and 'L2 (Layer 2)' (disabled). Other fields include 'HTTP Listening port: 8080', 'Proxy server: [text box]', 'Port: 8080', 'Port Number: 8081', 'Router IP address(es): admin', and 'Password: [masked]'. There are 'Save' and 'Cancel' buttons at the bottom.

Dans le cas d'une implémentation existante avec deux passerelles Trend InterScan Web Security configurées avec les rôles de serveurs Parent ou Enfant, il conviendra de désactiver cette fonctionnalité sur les passerelles comme indiqué ci-dessous.

The screenshot shows the configuration page for the Trend Micro InterScan Web Security Virtual Appliance, specifically the 'Server Configuration' section. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Server Configuration' and has a single checkbox 'Enable for use in a multiple IWSVA server configuration' which is unchecked. Below this, there are fields for 'Parent's listening port number: 1444', 'Server role: Parent server' (selected), and 'Parent's IP address: [text box]'. There are 'Save' and 'Cancel' buttons at the bottom.

OBJECTIF

Répartir la charge et assurer la haute disponibilité des passerelles de filtrage et anti-malwares Trend InterScan Web Security afin d'en optimiser les performances.

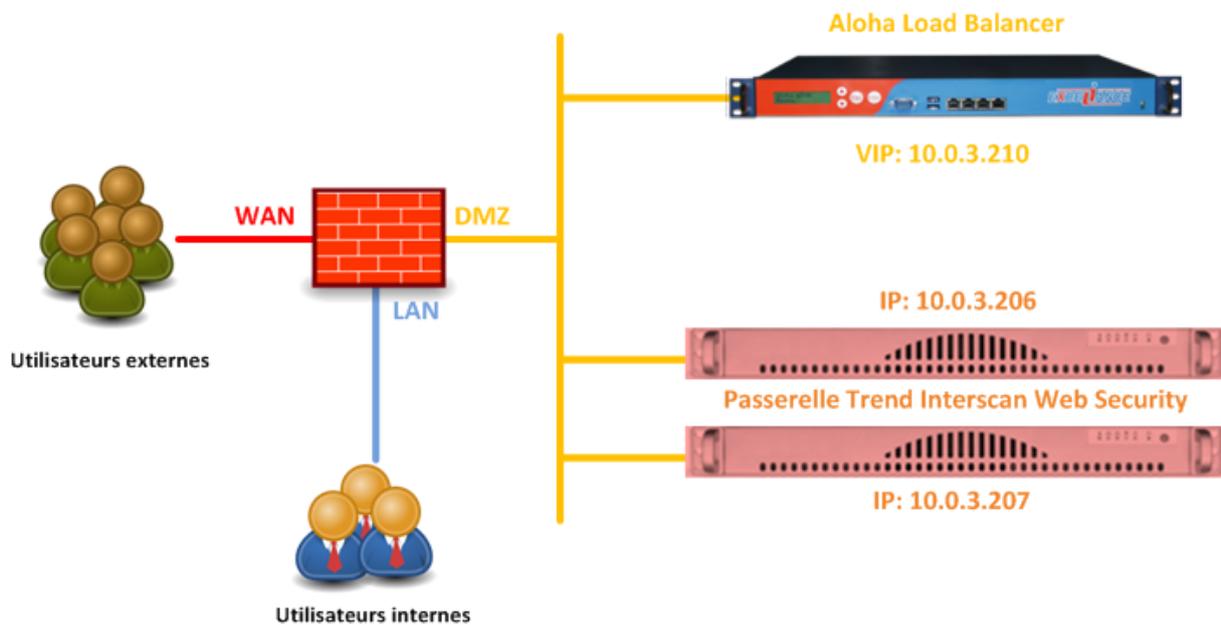
COMPLEXITE



VERSIONS CONCERNEES

V 3.x et ultérieures

SCHEMA CIBLE



EXTRAIT DE LA CONFIGURATION LB NIVEAU 7

```
##### The first public address as seen by the clients
frontend ft_TrendWEB
  bind 10.0.3.210:8080 # address:port to listen to
  mode http
  option http-use-proxy-header
  log global # use global log parameters
  option httplog # Enable HTTP logging
  maxconn 1000 # max conn per instance
  timeout client 25s # maximum client idle time
  default_backend bk_TrendWEB # send everything to this backend
```

```
##### backend bk_TrendWEB manages the servers and the load balancing algorithm
backend bk_TrendWEB
    balance uri # source | roundrobin | uri | leastconn
    hash-type consistent
    mode http
    stats uri /stats
    stats show-legends
    stats show-node
    option forwardfor except 127.0.0.1/8 # add X-Forwarded-For except local
    log global
    option httpchk OPTIONS / HTTP/1.0\r\nhost:\ 0.0.0.0:8080 # HTTP check method
    option httplog # Enable HTTP logging
    fullconn 1000 # dynamic limiting below
    timeout server 25s # max server's response time
    default-server inter 3s rise 2 fall 3 slowstart 0 # servers default parameters
    server TrendWEB1 10.0.3.206:8080 weight 10 maxconn 1000 check # TrendWEB1 config
    server TrendWEB2 10.0.3.207:8080 weight 10 maxconn 1000 check # TrendWEB2 config
```

Avec :

bind 10.0.3.210:8080 : adresse IP et port d'écoute.

option http-use-proxy-header : à utiliser lors de connexions avec un Proxy dont les en-têtes sont non standard (cf RFC2616).

balance uri : permet d'affecter toujours la même uri sur le même serveur, en appliquant un hash de la partie gauche de l'uri (avant le point d'interrogation) puis en divisant le résultat par le total des poids des serveurs actifs.

hash-type consistent : permet de spécifier que le hachage est dynamique, il prend en charge l'évolution des poids pendant que les serveurs sont en place, il est donc compatible avec la fonction de démarrage lent. Il offre l'avantage que lorsqu'un serveur change d'état et devient indisponible, ses associations sont déplacées sur un autre.

option httpchk OPTIONS / HTTP/1.0\r\nhost:\ 0.0.0.0:8080 # HTTP check method : permet de faire un check d'état sur le port 8080.

server TrendWEB1 10.0.3.206:8080 weight 10 maxconn 1000 check # TrendWEB1 config : permet de spécifier la passerelle Trend de destination (son IP, son port, son poids dans la ferme...)

server TrendWEB2 10.0.3.207:8080 weight 10 maxconn 1000 check # TrendWEB2 config : permet de spécifier la passerelle Trend de destination (son IP, son port, son poids dans la ferme...)