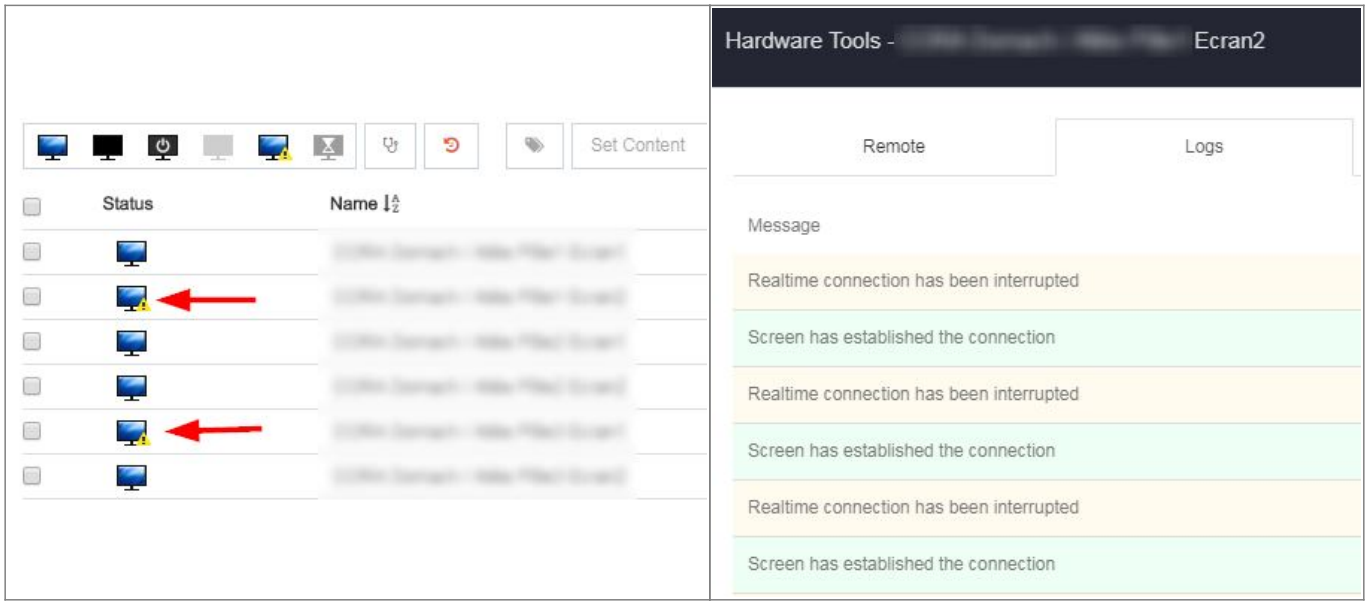
Comment éviter les « connexions instables »

Pourquoi cela se produit-il ?



Vous avez peut-être remarqué que certains écrans affichent l'avertissement « connexion instable ». Cette situation se produit lorsque le canal de communication en temps réel entre l'écran et le serveur est interrompu. La communication en temps réel est nécessaire pour obtenir l'état de l'écran ou d'autres informations, ainsi que pour envoyer des commandes à l'écran (allumer, éteindre, changer le contenu, obtenir une capture d'écran, redémarrer, etc.). La principale cause de ce problème est la configuration du pare-feu, et dans la plupart des cas, le problème peut être facilement résolu.

Première tentative de correction à effectuer

Nous avons constaté qu'avec certains pare-feux / routeurs ou fournisseurs d'accès Internet (FAI), le problème pouvait facilement être résolu en passant la connexion de l'écran à Zebrix en HTTPS au lieu de HTTP.

Sur un écran SAMSUNG, vous devez modifier l'URL, par exemple passer de http://screen.zebrix.net à https://screenv2.zebrix.net. Voici comment modifier l'URL sur un écran SAMSUNG

Sur un lecteur Zebrix, vous devez ouvrir l'outil de configuration et sélectionner https au lieu de http dans la section « protocole ». Voici comment ouvrir l'outil de configuration sur un lecteur Zebrix

D'après notre expérience, ce problème a souvent été signalé avec les FAI PROXIMUS (Belgique) et TELENET (Belgique). Nous n'avons pas pu identifier la cause exacte de ce problème : nous ne savons pas s'il provient du réseau de ces FAI ou du modem/routeur/pare-feu fourni par ceux-ci.

Pare-feux connus pour être concernés par ce problème + solutions

Fortinet Fortigate

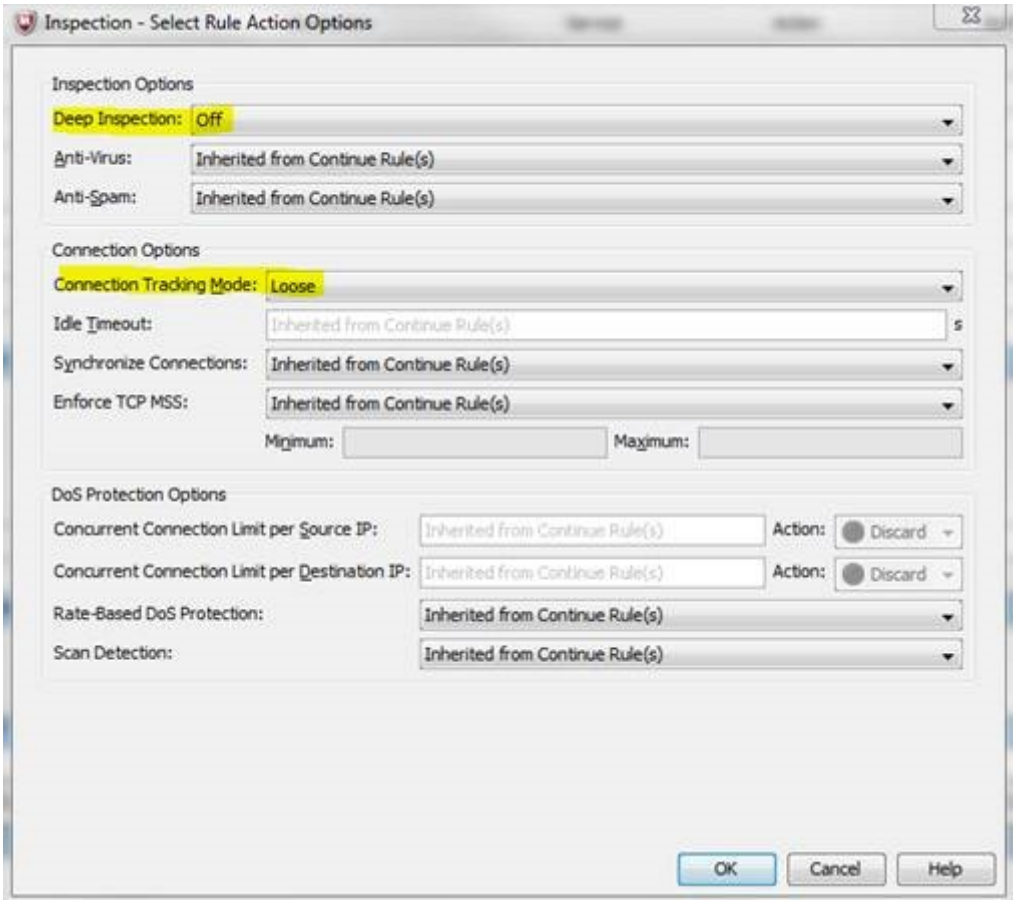
Les pare-feux Fortigate ont un paramètre par défaut fixant à 5 minutes la durée de vie (TTL) des sessions TCP ; les sessions actives sans activité de paquets sont simplement coupées. Ce paramètre ne peut pas être modifié via l'interface web — il faut utiliser le CLI. Voici un exemple pour ajuster le TTL à 86400 secondes pour la règle concernée, avec une valeur par défaut de 10 minutes pour le reste :

```
config system session-ttl
set default 600
config port
edit 123
set protocol 6
set timeout 86400
set end-port 80
set start-port 80
next
end
end
```

Le « 123 » après la commande edit correspond simplement au numéro de la règle ; il n'a aucun lien avec le port, qui est défini dans la règle comme une plage. Le protocole 6 correspond au TCP.

Stonesoft

Le problème sur les pare-feux Stonesoft peut être facilement corrigé en désactivant la fonction « Deep Inspection » et en changeant le mode de suivi de connexion (« Connection tracking mode ») sur « Loose ».



Bluecoat Proxy / Firewall

Il a été constaté que le module antivirus du proxy Bluecoat ferme régulièrement le canal de communication afin d'effectuer ses analyses. Si désactiver l'antivirus n'est pas une option, il est recommandé de passer la connexion des écrans en HTTPS au lieu de HTTP, ce qui résout généralement le problème.

Autres pare-feux ?

Veuillez envisager d'ajuster ou de désactiver les modules suivants dans la règle créée pour Zebrix :

Module antivirus HTTP

WebFilter / ContentFiltering

Module DLP

SSL Inspection

Deep Packet Inspection

Connection Tracking

Proxy transparent

Ajustement du TTL (Time-to-Live) ou du délai d'expiration (Timeout)

En alternative, vous pouvez également essayer d'utiliser HTTPS au lieu de HTTP, ou HTTP sur TCP6001 au lieu de HTTP sur TCP80 (certains pare-feux peuvent être plus permissifs sur ce port).