Distribution EOLE - Tâche #19686

Scénario # 19382 (Terminé (Sprint)): Traitement express MEN (10-12)

ERA/bastion doit pouvoir supporter un nom de modèle avec des accents

15/03/2017 09:46 - Olivier FEBWIN

Statut:	Fermé	**Début:**	15/03/2017
Priorité:	Normal	**Echéance:**	
Assigné à:	Fabrice Barconnière	**% réalisé:**	100%
Version cible:	sprint 2017 10-12 Equipe MENSR	**Temps estimé:**	2.00 heures
		Temps passé:	3.50 heures

Description

Sur Amon 2.5.2, un nom de modèle avec accent provoque une erreur à la génération du firewall

Pour reproduire :

```
root@amon:~# rm /etc/eole/iptables

root@amon:~# cp /usr/share/era/modeles/4zones.xml /usr/share/era/modeles/4zones-école.xml

root@amon:~# CreoleSet type_amon 4zones-école

root@amon:~# service bastion restart
 * Réinitialisation du pare-feu
 * Activation du mode forteresse sur eth0
 * Activation du mode forteresse sur eth1
 * Activation du mode forteresse sur eth2
 * Activation du mode forteresse sur eth3
   ...done.
 * Regénération des règles de pare-feuroot - 'ascii' codec can't encode character u'\xe9' in posit
ion 7: ordinal not in range(128)
   ...done.
 * Mise en cache des règles de pare-feu
   ...done.
 * Restauration des règles de pare-feu en cache
   ...done.
Réseau Virtuel Privé Non Configuré

root@amon:~# cat /etc/eole/iptables
# Generated by iptables-save v1.4.21 on Mon Mar 20 08:18:57 2017
*mangle
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
COMMIT
# Completed on Mon Mar 20 08:18:57 2017
# Generated by iptables-save v1.4.21 on Mon Mar 20 08:18:57 2017
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
COMMIT
# Completed on Mon Mar 20 08:18:57 2017
# Generated by iptables-save v1.4.21 on Mon Mar 20 08:18:57 2017
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
```

```
-A INPUT -i lo -j ACCEPT
-A INPUT -i eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
COMMIT
# Completed on Mon Mar 20 08:18:57 2017
```

Demande originale :

Ce matin, 2 établissements nous ont signalé que leur VPN n'était plus fonctionnel.
En jetant un oeil dans "afficher les logs complets" sur la page des serveurs concernés dans Zéphir on a toutes les 3 minutes "agent rvp : bastion arrêté, on ne relance pas rvp".

Sur ces Amon 2.5.2, un *service bastion status* renvoie : * Bastion n'est pas démarré : fichier lock non présent
[fail]

Révisions associées

Révision b660ff86 - 20/03/2017 10:54 - Fabrice Barconnière

Correction plantage **checkval** avec accent + test unitaire

ref #19686 @1h

Révision d80770d6 - 20/03/2017 11:03 - Fabrice Barconnière

Support des caractères accentués pour la génération du firewall

ref #19686 @30m

Révision a8318d37 - 20/03/2017 11:08 - Fabrice Barconnière

Support des caractères accentués pour la génération du firewall

ref #19686 @30m

Révision 9511124c - 22/06/2017 09:02 - Fabrice Barconnière

Revert "Support des caractères accentués pour la génération du firewall"
suite au merge de issue/20788
Supporté nativement par Creole ref #19686

This reverts commit a8318d377a6c76c2329f23a05a88febc5ca3c262.

Historique

#1 - 15/03/2017 10:23 - Olivier FEBWIN

- Fichier bastion.info.log ajouté

- Fichier zephiragents.info.log ajouté

#2 - 15/03/2017 10:29 - Olivier FEBWIN

ça pourrait bien être en relation avec #18328

#3 - 15/03/2017 10:32 - Olivier FEBWIN

et certainement depuis https://dev-eole.ac-dijon.fr/projects/modules-eole/wiki/Journaux252#23112016-Mise-%C3%A0-jour-corrective

#4 - 17/03/2017 15:57 - Fabrice Barconnière

- Statut changé de Nouveau à En attente d'informations

- Assigné à mis à Fabrice Barconnière

Il est normal que l'agent ne relance pas le VPN si bastion est arrêté.
Ce qui n'est pas normal, c'est que bastion ne le relance pas suite au logrotate d'après ce que je vois dans les logs.

Les règles iptables du modèle ERA sont-elles en place après le logrotate quand le VPN n'est pas relancé ?

Je pense que non, car il n'y a plus le **lock/bastion**, ce qui indique à l'agent de ne pas relancer le VPN.

#5 - 17/03/2017 16:05 - Fabrice Barconnière

- Fichier guardian.logrotate.patch ajouté

Au logrotate, **CreoleRun "service bastion restart" root no yes >/dev/null** régénère les règles iptables du modèle.
Cela prend du temps et peut poser problème si des services (comme un DNS forward, ...) sont inaccessibles à ce moment.
De plus, c'est inutile à ce moment là. La restauration du cache est suffisante.
Le régénération des règles se fait pendant le reconfigure.
Peux-tu essayer ce patch : guardian.logrotate.patch ?
Et faire un retour.

Merci

#6 - 17/03/2017 16:08 - Fabrice Barconnière

J'ai même l'impression (peut-être fausse) qu'il y a un problème sur le modèle ERA.
Que donne **service bastion restart** ?

#7 - 17/03/2017 16:26 - Olivier FEBWIN

effectivement il semble qu'il y ait un problème à ce niveau

```
root@0601864a-amon25:~#  service bastion restart
 * Réinitialisation du pare-feu
                                                                                                  * Activa
tion du mode forteresse sur eth0
                                                                                              * Activation du m
ode forteresse sur eth1
                                                                                          * Activation du mode forte
resse sur eth2
                                                                                      * Activation du mode forteresse sur
 eth3
                                                                              * Activation du mode forteresse sur eth4

                                                [ OK ]
 * Regénération des règles de pare-feu (modèle "5zones")version du 19/01/17 Autorisation du nouveau serveur Ca
rnet
root - 'ascii' codec can't encode character u'\xe9' in position 3: ordinal not in range(128)

************************************************************
vendredi 17 mars 2017, 16:23:37 (UTC+0100)
```

```
Reconfigure en cours sur l'amon 2.5.2 en variante "Lycée 5 zones"
 (0601864A)

id Zéphir : 780

Nom de la machine : 0601864a-amon25
eth0 = 10.66.5.240
eth1 = 10.60.84.240
eth2 = 172.16.0.1
eth3 = 10.160.84.240
eth4 = 192.168.254.240
*****************************************************************

Autorisation des IP autorisées à se connecter sur le VLAN vidéosurveillance eth1.20
Mise en place des règles pour les affranchisseuses Néopost
Mise en place des règles pour les TPE de paiement de la bourse aux livres (dont la nouvelle IP 2016)

###### MATRICE DES FLUX LYCÉES (INFRA 2015) ######
Blocage des flux production > management (sauf pour les retours)
Mise en place des règles pour RNE-SECU (zone management > gestion)
Mise en place des règles pour RNE-SECU (zone DMZ > management)
Mise en place des règles pour RNE-SVM (zone DMZ > management)
Mise en place des règles pour l'intégration au domaine des machines en DMZ (zone DMZ > management)
Mise en place des règles pour la supervision (zone management > gestion)
Mise en place des règles pour la supervision (zone management > production)
Mise en place des règles pour System Center (zone DMZ > management)
Mise en place des règles pour Pronote.NET > Pronote (zone DMZ > management)
Mise en place des règles pour rebond sur les interfaces web de switchs en zone management via Rinetd installé
sur le serveur Horus (zone Gestion > management)
###### FIN MATRICE DES FLUX LYCÉES (INFRA 2015) ######

Mise en place des règles pour la synchro BCDI web
Mise en place des règles pour la visioconférence
Redémarrage du réseau...
Removed VLAN -:eth1.20:-
ssh start/running, process 36210
ssh start/running, process 36284
Set name-type for VLAN subsystem. Should be visible in /proc/net/vlan/config
Added VLAN with VID == 20 to IF -:eth1:-
ssh start/running, process 36441
ssh start/running, process 36505
ssh start/running, process 36570
rsyslog stop/waiting
rsyslog start/running, process 36610
ssh start/running, process 36655
ssh start/running, process 36719
ssh start/running, process 36783
ssh start/running, process 36847
ssh start/running, process 36911
ssh start/running, process 36975
ssh start/running, process 37039
Réseau redémarré
Starting strongSwan 5.1.2 IPsec [starter]...
charon is already running (/var/run/charon.pid exists) -- skipping daemon start
starter is already running (/var/run/starter.charon.pid exists) -- no fork done
Aucune personnalisation des règles pour cet établissement -> Application des règles standards
Gestion poste : erreur à la mise en place des restrictions de postes/destinations (/sbin/iptables -I FORWARD -
i eth2 -s http://boogiewoogiekid.com/cgi-bin -j REJECT): , iptables v1.4.21: invalid mask `cgi-bin' specified
Try `iptables -h' or 'iptables --help' for more information.
Gestion poste : erreur à la mise en place des restrictions de postes/destinations (/sbin/iptables -i eth2 -I I
NPUT -s http://boogiewoogiekid.com/cgi-bin -j REJECT): , iptables v1.4.21: invalid mask `cgi-bin' specified
Try `iptables -h' or 'iptables --help' for more information.
Gestion poste : erreur à la mise en place des restrictions de postes/destinations (/sbin/iptables -I FORWARD -
i eth2 -d http://boogiewoogiekid.com/cgi-bin -j REJECT): , iptables v1.4.21: invalid mask `cgi-bin' specified
Try `iptables -h' or 'iptables --help' for more information.
Gestion poste : erreur à la mise en place des restrictions de postes/destinations (/sbin/iptables -I INPUT -i
eth2 -s http://boogiewoogiekid.com/cgi-bin -j REJECT): , iptables v1.4.21: invalid mask `cgi-bin' specified
Try `iptables -h' or 'iptables --help' for more information.

                                                                                [ OK ]
 * Mise en cache des règles de pare-feu
                                                                                [ OK ]
 * Restauration des règles de pare-feu en cache
                                                                                [ OK ]
 * Arret du Reseau Virtuel Privé
```

```
                                                                                [ OK ]
 * Lancement du Reseau Virtuel Privé
                                                                                [ OK ]
root@0601864a-amon25:~#
```

#8 - 17/03/2017 17:00 - Olivier FEBWIN

Comment puis-je trouver d'où vient l'erreur

```
root - 'ascii' codec can't encode character u'\xe9' in position 3: ordinal not in range(128)
```

?

#9 - 17/03/2017 17:00 - Olivier FEBWIN

pour les

```
Gestion poste : erreur à la mise en place des restrictions de postes/destinations (/sbin/iptables -I FORWARD -
i eth2 -s http://boogiewoogiekid.com/cgi-bin -j REJECT): , iptables v1.4.21: invalid mask `cgi-bin' specified
Try `iptables -h' or 'iptables --help' for more information.
Gestion poste : erreur à la mise en place des restrictions de postes/destinations (/sbin/iptables -i eth2 -I I
NPUT -s http://boogiewoogiekid.com/cgi-bin -j REJECT): , iptables v1.4.21: invalid mask `cgi-bin' specified
Try `iptables -h' or 'iptables --help' for more information.
Gestion poste : erreur à la mise en place des restrictions de postes/destinations (/sbin/iptables -I FORWARD -
i eth2 -d http://boogiewoogiekid.com/cgi-bin -j REJECT): , iptables v1.4.21: invalid mask `cgi-bin' specified
Try `iptables -h' or 'iptables --help' for more information.
Gestion poste : erreur à la mise en place des restrictions de postes/destinations (/sbin/iptables -I INPUT -i
eth2 -s http://boogiewoogiekid.com/cgi-bin -j REJECT): , iptables v1.4.21: invalid mask `cgi-bin' specified
Try `iptables -h' or 'iptables --help' for more information.
```

il s'agissait d'une mauvaise saisie dans l'EAD

#10 - 17/03/2017 17:30 - Olivier FEBWIN

Trouvé !
C'est

```
echo -e "\n\n*****************************************************************\n`date`\nReconfigure en cours
sur l'`CreoleGet eole_module` `CreoleGet eole_release` en variante \"Lycée 5 zones\"\n`CreoleGet libelle_etab`
 (`CreoleGet numero_etab`) \n\nid Zéphir : `ls /usr/share/zephir/monitor/data/config*|cut -d g -f2|cut -d . -f
1`\n\nNom de la machine : `CreoleGet nom_machine`\neth0 = `CreoleGet adresse_ip_eth0` \neth1 = `CreoleGet adre
sse_ip_eth1`\neth2 = `CreoleGet adresse_ip_eth2`\neth3 = `CreoleGet adresse_ip_eth3`\neth4 = `CreoleGet adress
e_ip_eth4`\n*****************************************************************\n"
```

#11 - 20/03/2017 08:27 - Fabrice Barconnière

- Tracker changé de Demande à Tâche

- Projet changé de Amon à ERA

- Sujet changé de Parfois bastion ne démarre pas à 6h30 sur Amon 2.5.2 > l'agent ne relance pas les VPN à ERA/bastion doit pouvoir supporter un nom de modèle avec des accents

- Description mis à jour

- Statut changé de En attente d'informations à Nouveau

- Temps estimé mis à 2.00 h

- Tâche parente mis à #19382

- Restant à faire (heures) mis à 2.0

#12 - 20/03/2017 08:29 - Fabrice Barconnière

- Projet changé de ERA à Distribution EOLE

- Description mis à jour

- Assigné à Fabrice Barconnière supprimé

#13 - 20/03/2017 09:36 - Olivier FEBWIN

le nom du modèle que j'utilise en comporte pas d'accent

#14 - 20/03/2017 10:27 - Fabrice Barconnière

- Statut changé de Nouveau à En cours

#15 - 20/03/2017 10:27 - Fabrice Barconnière

- Assigné à mis à Fabrice Barconnière

#16 - 20/03/2017 11:13 - Fabrice Barconnière

- % réalisé changé de 0 à 100

- Restant à faire (heures) changé de 2.0 à 0.5

Corrigé en 2.5.1, 2.5.2 (même correctif, uniquement le script init **bastion**) et 2.6.1 (corrigé dans creole avec test unitaire).

#17 - 20/03/2017 11:44 - Gwenael Remond

- Statut changé de En cours à Fermé

- Restant à faire (heures) changé de 0.5 à 0.0

#18 - 20/03/2017 11:57 - Fabrice Barconnière

- Statut changé de Fermé à Résolu

- Restant à faire (heures) changé de 0.0 à 0.5

#19 - 21/03/2017 09:36 - Scrum Master

- Statut changé de Résolu à Fermé

- Restant à faire (heures) changé de 0.5 à 0.0

#20 - 22/03/2017 09:04 - Olivier FEBWIN

- Fichier Capture du 2017-03-22 08-50-41.png ajouté

Encore 6 problèmes de VPN sur les amon 2.5.2 ce matin à cause de ce problème de bastion.
Les règles de pare-feu sont bien en place.

#21 - 29/03/2017 09:40 - Olivier FEBWIN

Je ne pense pas que mon problème vienne d'un problème d'accent dans le nom du modèle .xml puisque celui-ci n'en contient pas...
J'essaie de faire une rustine en essayant de relancer bastion par cron s'il est arrêté mais ça ne fonctionne pas.
Voici ce que j'ai placé dans /etc/cron.d/relance_bastion :

```
0 7  * * *   root if [ -f /var/run/lock/bastion ]; then echo "`date` : Le verrou /var/run/lock/bastion est pré
sent ; on ne relance pas bastion" >> /var/log/syslog; else echo -e "`date` : Le verrou /var/run/lock/bastion n
'est pas présent ; on relance bastion !" >> /var/log/syslog; /usr/bin/CreoleService bastion restart; fi;
```

#22 - 29/03/2017 10:21 - Olivier FEBWIN

il me manquait

```
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
```

Fichiers

bastion.info.log	3,77 ko	15/03/2017	Olivier FEBWIN
zephiragents.info.log	30,7 ko	15/03/2017	Olivier FEBWIN
guardian.logrotate.patch	407 octets	17/03/2017	Fabrice Barconnière
Capture du 2017-03-22 08-50-41.png	170 ko	22/03/2017	Olivier FEBWIN