

SecurityFocus SUN: Sunscreen cluster: "You must log in before using the sys_info command"

Sunscreen cluster: "You must log in before using the sys_info command"

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-sun/2003-11/0017.html>

From: Sean Boran (sean_at_boran.com)

Date: 11/26/03

To: <focus-sun@securityfocus.com>

Date: Wed, 26 Nov 2003 08:22:12 +0100

Hi,

I want to convert a running Sunscreen 3.2 firewall to a cluster. I've experimented with secondary and primaries in the lab and got the clustering working.

However on the live system, I'm having problems.

After doing on the secondary:

```
ssadm ha init_secondary eri1 172.17.17.204
```

I do the usual on the primary:

```
ssadm ha add_secondary 172.17.17.203
```

The secondary machine (fw3b) has been added to the HA cluster.

Activate your policy to activate the secondary machine.

which works fine. The two systems can ping each other over the HB interface, eri1, which is a simple crossover cable.

When I activate the policy though there are communication problems with the secondary:

```
ssadm activate mypolicy
```

```
Synchronizing configurations on fw3b
```

```
ssadm: Can't run command: java.io.IOException: Error from remote server:
```

```
You must log in before using the sys_info command.
```

```
Warning: HA host fw3b is not responding.
```

```
Configuration synchronized on HA cluster.
```

```
SunScreen HA Screen becoming ACTIVE Screen.
```

```
Configuration activated successfully on fw3.
```

```
root@fw3:~[26]$ SunScreen HA Screen entering PASSIVE mode.
```

```
SunScreen HA Screen becoming ACTIVE Screen.
```

If I run a snoop on eri1 of fw3b, I see HA port traffic:

```
fw3_ha -> fw3b_ha TCP D=3853 S=32810 Syn Seq=3992249057 Len=0
```

```
Win=49640 Options=<mss 1460,nop,nop,sackOK>
```

```
fw3b_ha -> fw3_ha TCP D=32810 S=3853 Syn Ack=3992249058
```

```
Seq=871156038 Len=0 Win=49640 Options=<mss 1460,nop,nop,sackOK>
```

```
fw3_ha -> fw3b_ha TCP D=3853 S=32810 Ack=871156039 Seq=3992249058
```

Sunscreen cluster: "You must log in before using the sys_info command"

SecurityFocus SUN: Sunscreen cluster: "You must log in before using the sys_info command"

```
Len=0 Win=49640
  fw3_ha -> fw3b_ha TCP D=3853 S=32810 Push Ack=871156039
Seq=3992249058 Len=112 Win=49640
  fw3b_ha -> fw3_ha TCP D=32810 S=3853 Ack=3992249170 Seq=871156039
Len=0 Win=49528
  fw3b_ha -> fw3_ha TCP D=32810 S=3853 Push Ack=3992249170
Seq=871156039 Len=68 Win=49528
  fw3b_ha -> fw3_ha TCP D=32810 S=3853 Fin Ack=3992249170
Seq=871156107 Len=0 Win=49528
  fw3_ha -> fw3b_ha TCP D=3853 S=32810 Ack=871156107 Seq=3992249170
Len=0 Win=49640
  fw3_ha -> fw3b_ha TCP D=3853 S=32810 Ack=871156108 Seq=3992249170
Len=0 Win=49640
  fw3_ha -> fw3b_ha TCP D=3853 S=32810 Fin Ack=871156108
Seq=3992249170 Len=0 Win=49640
  fw3b_ha -> fw3_ha TCP D=32810 S=3853 Ack=3992249171 Seq=871156108
Len=0 Win=49528
```

Even when not activating a policy, there is constant HB traffic:

```
fw3b_ha -> (broadcast) ARP C Who is 172.17.17.204, fw3_ha ?
fw3_ha -> fw3b_ha ARP R 172.17.17.204, fw3_ha is 0:3:ba:13:85:9b
fw3b_ha -> fw3_ha ICMP Echo reply (ID: 1259 Sequence number:
41978)
fw3_ha -> fw3b_ha ICMP Echo request (ID: 1259 Sequence number:
41979)
fw3b_ha -> fw3_ha ICMP Echo reply (ID: 1259 Sequence number:
41979)
fw3_ha -> fw3b_ha ICMP Echo request (ID: 1259 Sequence number:
41980)
fw3b_ha -> fw3_ha ICMP Echo reply (ID: 1259 Sequence number:
41980)
fw3_ha -> fw3b_ha ICMP Echo request (ID: 1259 Sequence number:
41981)
fw3b_ha -> fw3_ha ICMP Echo reply (ID: 1259 Sequence number:
41981)
```

Any ideas what could be wrong? I deleted certificates on the secondary and re-ran ssadm configure, just to be sure. I also added a rule on each screen to allow traffic on eri0 between both systems. No luck though..

Thanks in advance,

Sean Boran