

RE: [fw-wiz] PIX 501 outgoing SMTP problem – (reset-o)

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2006-04/msg00022.html>

- *From:* "Sanford Reed" <sanford.reed@xxxxxxx>
 - *Date:* Fri, 7 Apr 2006 15:31:40 -0400
-

Cameron

It sounds like that Email Server has been updated and is now using Extended Simple Mail Transfer Protocol (ESMTP). Even with Mailguard off I had problems getting a 515E to pass those packets. Google the terms esmtp pix and you will find several possible fixes. IF you have a Cisco Tac login here is a link discussing the problem.

<http://www.ciscotaccc.com/security/showcase?case=K11355672>

-----Original Message-----

From: firewall-wizards-admin@xxxxxxxxxxxxxxxxxxxxx

[<mailto:firewall-wizards-admin@xxxxxxxxxxxxxxxxxxxxx>] On Behalf Of Cameron

Matheson

Sent: Wednesday, April 05, 2006 10:41 AM

To: firewall-wizards@xxxxxxxxxxxxxxxxxxxxx

Subject: [fw-wiz] PIX 501 outgoing SMTP problem – (reset-o)

Hi

Starting about three weeks ago, some outbound emails stopped flowing properly (large emails to some domains with ip addresses very close to ours were not being delivered). Inbound email is fine. The PIX (version 6.3(3)) syslog messages looked like this:

```
3/31/2006 19:38 built outbound tcp connection 268422 for
outside:<RecipientMailserverIP>/25 (<RecipientMailserverIP>/25) to
inside:<ExchangeServerPrivateIP>/9112 (<OurOutsideIP>/34960)
3/31/2006 19:39 teardown tcp connection 268422 for
outside:<RecipientMailserverIP>/25 to inside:<ExchangeServerPrivateIP>/9112
duration 0:01:04 bytes 36129 tcp reset-o
3/31/2006 19:39 inbound tcp connection denied from
<RecipientMailserverIP>/25 to <OurOutsideIP>/34960 flags rst on interface
outside
3/31/2006 19:39 deny tcp (no connection) from
<ExchangeServerPrivateIP>/9112 to <RecipientMailserverIP>/25 flags ack on
interface inside
```

Further examination of the Exchange Server smtp logs shows that the smtp

RE: [fw-wiz] PIX 501 outgoing SMTP problem – (reset-o)

RE: [fw-wiz] PIX 501 outgoing SMTP problem – (reset-o)

conversation was not completing ...

```
199.246.2.14 – OutboundConnectionResponse [31/Mar/2006:19:38:45 -0500] "-
-?220+mailgate1.kos.net SMTP" 0 21
199.246.2.14 – OutboundConnectionCommand [31/Mar/2006:19:38:45 -0500] "HELO
-?exchange.OURDOMAIN SMTP" 0 4
199.246.2.14 – OutboundConnectionResponse [31/Mar/2006:19:38:45 -0500] "-
-?250+mailgate1.kos.net SMTP" 0 21
199.246.2.14 – OutboundConnectionCommand [31/Mar/2006:19:38:45 -0500] "MAIL
-?FROM:<someone@xxxxxxxxxxxxxx> SMTP" 0 4
199.246.2.14 – OutboundConnectionResponse [31/Mar/2006:19:38:45 -0500] "-
-?250+Ok SMTP" 0 6
199.246.2.14 – OutboundConnectionCommand [31/Mar/2006:19:38:45 -0500] "RCPT
-?TO:<someone@xxxxxxxxxxxxxx> SMTP" 0 4
199.246.2.14 – OutboundConnectionResponse [31/Mar/2006:19:38:45 -0500] "-
-?250+Ok SMTP" 0 6
199.246.2.14 – OutboundConnectionCommand [31/Mar/2006:19:38:45 -0500] "DATA
- SMTP" 0 4
199.246.2.14 – OutboundConnectionResponse [31/Mar/2006:19:38:45 -0500] "-
-?354+End+data+with+<CR><LF>.<CR><LF> SMTP" 0 35
```

There should be more lines after this one to show that the email was sent successfully. They should look like this:

```
199.246.2.14 – OutboundConnectionResponse [03/Apr/2006:10:15:41 -0500] "-
-?250+Ok:+queued+as+5071BD01049B SMTP" 0 30
199.246.2.14 – OutboundConnectionCommand [03/Apr/2006:10:15:41 -0500] "QUIT
- SMTP" 0 4
199.246.2.14 – OutboundConnectionResponse [03/Apr/2006:10:15:41 -0500] "-
-?221+Bye SMTP" 0 7
```

Does this mean anything to you? Is the reset-o significant? Or is it the inbound tcp connection denied that is the problem?

On Saturday I upgraded the firmware on our PIX 501 firewall to 6.3(5) and checked the configuration to be certain that the "Mailguard" feature was disabled. (no fixup protocol smtp 25) Still no improvement, so I replaced the PIX firewall by a Linksys router as a test, and email flowed perfectly! Then, I put the PIX back in place and went home. On Monday morning, mail was flowing perfectly through the PIX and is still fine today (Tuesday). So I'm not sure if the firmware upgrade solved the problem or if it was something else. Our ISP claims that they did not change anything over the weekend, but now the SMTP conversation completes properly and the firewall reports:

```
4/3/2006 10:15 built outbound tcp connection 2309 for
outside:<RecipientMailserverIP>/25 (<RecipientMailserverIP>/25) to
inside:<ExchangeServerPrivateIP>/26715 (<OurOutsideIP>/2133)
4/3/2006 10:15 teardown tcp connection 2309 for
outside:<RecipientMailserverIP>/25 to inside:<ExchangeServerPrivateIP>/26715
duration 0:00:10 bytes 5212799 tcp fins
```

RE: [fw-wiz] PIX 501 outgoing SMTP problem – (reset-o)

RE: [fw-wiz] PIX 501 outgoing SMTP problem – (reset-o)

I would love to know for sure if the problem is really fixed, or will it come back? Is there something wrong with my PIX configuration? Do you have any ideas?

Thanks again for all your help.

cmatheson@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

firewall-wizards mailing list
firewall-wizards@xxxxxxxxxxxxxxxxxxxxx
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>

firewall-wizards mailing list
firewall-wizards@xxxxxxxxxxxxxxxxxxxxx
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>