
From: badra@isima.fr
Sent: Tuesday, October 9, 2007 6:05 PM
To: ngo@ietf.org; netconf@ops.ietf.org
Cc: simon@switch.ch
Subject: [NGO] NETCONF over TLS document (Proposed Re-charting of NETCONF WG)

[Apologies for multiple reception]

Dear all,

I submitted a new version of "NETCONF over TLS" that (Staging URL:
<http://www3.ietf.org/proceedings/staging/draft-badra-tls-netconf-04.txt>):

a) includes comments from Eric Rescorla since I asked Eric to review the document (his comments are given below).
Thanks Eric.

b) supports the Notification draft (the <notification> elements are also mentioned).

As the NETCONF WG re-chartering is discussed right now and since some documents are currently not considered in scope for re-charting at this time, I'd hope there will be consensus to take on the document and I'd like to have more comments and discussion on the document for adoption as WG item.

Best regards,
Badra

===== Eric Rescorla review =====

\$Id: draft-badra-tls-netconf-03-rev.txt,v 1.1 2007/10/08 16:31:02 ekr Exp \$

This draft seems conceptually sound. That said, the NETCONF WG made a deliberate decision to use SSH rather than TLS. I don't fully understand why they made that decision, but I wonder how receptive they are going to be to a TLS proposal.

I see a bunch of SHOULDs that really should be MUSTs. In particular, TLS requires clarity about which side is which, so in S 2.1. where you talk about which side is the client and which the server, these should be MUST.

When a party has received the close_notify alert from the other party and still has pending data to send, it SHOULD send the pending data before sending the close_notify alert.

This violates RFC 4346:

Unless some other fatal alert has been transmitted, each party is required to send a close_notify alert before closing the write side of the connection. The other party MUST respond with a close_notify alert of its own and close down the connection immediately, discarding any pending writes. It is not required

for the initiator of the close to wait for the responding
close_notify alert before closing the read side of the connection.

ISTM that the security considerations here could use some work. What are the security guarantees required, esp. for upper-level authentication.

===== The review end=====

NGO mailing list
NGO@ietf.org
<https://www1.ietf.org/mailman/listinfo/ngo>