Advisory: NAPTR records - Improving Efficiency of International Authentication through utilisation of RadSec at National Level

October 2012 (3/10/2012)

Updated 2/11/2023

This advisory is relevant to ALL Home (IdP) service organisations participating in eduroam in the UK. It describes the use of RadSec at national proxy level, how this can benefit the individual user and what eduroam organisations must do in order to gain these benefits.

*****This Advisory Remains in Force - it is Applicable to the Current Date*****

Originator: Alan Buxey

Abstract

This article is relevant to ALL Home (IdP) service organisations participating in eduroam in the UK. It describes the use of RadSec at national proxy level, how this can benefit the individual user and what eduroam organisations must do in order to gain these benefits. The aim of this RadSec initiative is to improve the efficiency and performance of authentication for roaming users when trying to connect to eduroam in other European countries. All that is needed are some additions to the configuration of the participating organisation's DNS zone file.

This advisory is a recommendation to implement a simple DNS configuration measure in order to support RadSec based authentication transactions at International level. It is not a recommendation to implement RadSec at organisational level. A number of constraints apply to the more widespread deployment of RadSec as described at the end of this article.

Introduction

The UK National RADIUS proxy servers have been operating with RadSec support (Dynamic Discovery as well as TLS over TCP) for some time and we have been conducting trials across Europe. We think it is now time to take advantage of RadSec and dynamic server discovery so that the number of RADIUS queries that have to traverse the top level international proxies (the European Top Level Radius servers) can be reduced and more efficient routing achieved.

How does it Work?

The efficiency improvement can be achieved because RadSec allows the national RADIUS

proxy servers at one NREN confederation member (National RADIUS Operator) to talk to another directly, bypassing the ETLRs. In order to achieve this RadSec checks NAPTR (Network Authority PoinTeR) resource records in DNS to determine where RADIUS packets must be sent using SRV (service records) for your domain/realm zone name.

In order to benefit from the efficiency gains made possible by the new national level RadSec implementation, the joy is that eduroam organisations do not have to support RadSec natively on the ORPS! This possible because although the inter-NREN authentication transaction will use RadSec Dynamic Discovery, the transactions between ORPS and NRPS will use standard RADIUS as a present. The RADIUS request is proxied from the visited country's national proxy server using RadSec and dynamic server discovery straight to the UK NRPS, which then accepts it (based on certificates in the RadSec transaction) and then passes it on to the ORPS directly using good old fashioned RADIUS.

In this way, users visiting e.g. Germany will get their requests sent from the German organisation's ORPS to the German NRPS and sent then directly to the UK - that results in 2 hops in each direction dropped from the path for every one of the packets transfered. Currently (updated Jan 2015) Belgium, Germany, Ireland, Luxembourg, Netherlands, Norway, Poland, Spain, Switzerland and the UK have deployed RadSec Dynamic Discovery, with Denmark and Sweden and others soon to follow suit.

For a little more information about RadSec, NAPTR, SRVs etc see https://wiki.geant.org/display/H2eduroam/DNS-NAPTR [1]

Instructions

How do you join the party? You simply need to define a NAPTR record that points (indirectly) to the required SRV records (which define the required UK NRPS).

a) Recommended method.

1) Define a NAPTR record for your zone that points to the Janet roaming _radsec._tcp. record in the main zone header section of your DNS, alongside the usual MX, TXT, SPF etc entries.

a) If you can directly edit your zone file: on a fresh line append the following to your realm name TTL and internet (IN) zone specifiers:

NAPTR 100 10 "s" "x-eduroam:radius.tls" "" _radsec._tcp.roaming.ja.net.

e.g. camford.ac.uk. 43200 IN NAPTR 100 10 "s" "x-eduroam:radius.tls" "" _radsec._tcp.roaming.ja.net.

Nb. Be careful - the above is case sensitive! (Except the 's' can be uppercase 'S' https://tools.ietf.org/html/rfc2915 [2] 'Flags are single characters from the set [A-Z0-9]. The case of the alphabetic characters is not significant.'

b) If you use a portal with a GUI to manage your zonefile, use the menu system to define a NAPTR record and the following to populate the fields:

Field	Value

Type	NAPTR
Order	100
Preference	10
Flags	s
Services	x-eduroam:radius.tls
Regexp (*)	
Replacement (**)	_radsec._tcp.roaming.ja.net
Class	IN
TTL	43200

(*) Value is NULL (blank)

(**) Some systems are a little fussy about the replacement and may not like the value beginning with an underscore, in which case please get back to us.

2) Verify your DNS entry - from linux command line run DIG on your domain or use a DNS lookup web service (e.g. https://dnslookup.online/ [3])

Using dig: $ dig +short -t naptr camford.ac.uk

Result:
100 10 "s" "x-eduroam:radius.tls" "" _radsec._tcp.roaming.ja.net.

That's it! (The _tcp records section of the ja.net zone file includes the required SRV records for the 3 NRPSs.)

Nb. If you have multiple realm names defined for eduroam, you must add a NAPTR records for all of your realms! That includes sub-realms too.

Nbb. If you run DNSSEC might want to prove that the SRVs are real and verified.

Organisations running DNSSEC can then have the happy feeling that all of this is 100% validated - but in this case it doesn't really matter as we are using a closed club (eduroam RadSec currently uses a special CA that only members can use to create the transaction)

NB. Some DNS Servers do not support NAPTR:

Windows Server 2003 DNS Server and Windows 2008 non-R2 DNS Server (all end of life!) CANNOT do NAPTR

Cloudpit (Dogado), djbdns (without a patch applied...which is unlikely to be in a distro release) CANNOT do NAPTR

DNS Servers which do support NAPTR:

AWS Route 53, Cloudflare (since Aug 2018), Windows Server 2008 R2 onwards, BIND, CNR,

PowerDNS, NSD, MaraDNS unxsbind and DNSmasq all CAN do it

Resources: NAPTR Record Creation using MS Windows 2008R2 [4]

Test Systems to Verify and Monitor Site Records

As of May 2013 a check for NAPTR records is part of the eduroam(UK) Nagios test system running on the Support server. An alert appears on the Nagios LG page and also on your main configuration page.

Constraints Limiting Wider RadSec Deployment

This advisory is a recommendation to implement a simple DNS configuration measure in order to support RadSec based authentication transactions at International level. It is not a recommendation to implement RadSec at organisational level for ORPS - NRPS communication. A major constraint is that RadSec, both TLS over TCP and Dynamic Server Discovery, is only supported at present in Radiator and RadSecProxy RADIUS implementations. RadSec TLS over TCP will be included in FreeRADIUS 3 and DD will become available in future releases.

If a RADIUS platform that supports RadSec has been deployed as the ORPS, participating organisations may implement (and we would recommend implemention of) RadSec TLS over TCP for communication with the national proxies. The NRPS are based on Radiator and so support TLS over TCP. Nb. Implementation requires the use of special eduroam-signed certificates - guidance on this is outside the scope of this advisory.

RadSec Dynamic Server Discovery is NOT permitted since an important and long standing tennet of the eduroam trust model (dating from the inception of the service) is that all RADIUS transactions pass through the NRPS. Only when a robust central logging system has been developed can direct organisation - organisation authentication be considered. On a practical level (at the time of writing), there were ongoing issues with DD on ALL of the platforms which at the time supported it (Radiator and radsecproxy).

Links
[1] https://wiki.geant.org/display/H2eduroam/DNS-NAPTR
[2] https://tools.ietf.org/html/rfc2915
[3] https://dnslookup.online/
[4] https://support.eduroam.uk/files/NAPTR%20on%20Windows%20Server%20R2_0.doc