

Re: shared SSL

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2002-12/6696.html>

From: Thomas Deml [Msft] (thomad@online.microsoft.com)

Date: 12/12/02

From: "Thomas Deml [Msft]" <thomad@online.microsoft.com>

Date: Wed, 11 Dec 2002 23:23:27 -0800

Robert,

I have to agree that this is kind of unfortunate. As you already mentioned, IIS always routes to the first site configured for SSL on a particular IP address. The UI allows you to configure multiple SSL sites on the same IP, but IIS would never route requests to a second site. Not even wildcard certs (*.domainname.com) would help, because the routing to a particular site is done before the cert is used for decryption. IIS would have to evaluate the request twice before it routes:

- 1) When the request comes in a cert has to be found for the IP:Port combination. The cert is used to decrypt the request.
- 2) When the request is decrypted the host-header becomes available (it came in encrypted) – now IIS can route to a host-header based site.

Again, unfortunately IIS doesn't work this way (yet). You need an IP address per SSL site. Another idea is to terminate SSL before it gets to IIS, e.g. with ISA Server. ISA then routes the decrypted request as HTTP request to IIS.

Hope this helps.

--

Thomas Deml

Lead Program Manager

Internet Information Services

Microsoft Corp.

"Karl Levinson [x y] mvp" <levinson_k@excite.com> wrote in message news:O#5337ToCHA.2440@TK2MSFTNGP11...

>

> "robik" <robik@mailbox.sk> wrote in message

> news:093d01c2a138\$bee5b1c0\$d7f82ecf@TK2MSFTNGXA14...

> > Hi!

> >

> > Does anybody know how to implement shared SSL on IIS5? In

> > IIS4 were a possibility to bind a certificate at the master

> > level, but in IIS5 i can bind e certificate only to a

> > specic website.

> >

> > I'm writing an ISAPI filter wich overwrites the host http

> > header. I place this filter behind the ssipfilt.dll wich

Re: shared SSL

microsoft.public.inetserver.iis.security: Re: shared SSL

> > does the ssl stuff, but the binding to the website
> > happens already in the ssipilt, so my change in the the
> > host http header has no effect.
>
> If I understand your question correctly, SSL has always been bound to the
> host name in the URL, no matter whether using IIS4, IIS5, Apache, etc. It
> is possible to request a cert that has a wildcard such as
> *.domainname.com,
> though I'm not sure whether all browsers and servers accept this.
>
> It is absolutely possible to use one cert for multiple virtual server
> sites
> at a certain domain such as <https://domain.com>,
> <https://domain.com/domain2>,
> <https://domain.com:444>, etc. etc. as long as the host name is the same
> [or
> the domain name is the same and a wild card was used when generating the
> cert].
>
> You can't use host headers to keep the SSL sites separate, but you can use
> host headers on a non-SSL root page and a different port number on the SSL
> sites, such as <http://domain1.com> which immediately redirects the users to
> the first SSL site <https://domain.com> and also <http://domain2.com> which
> then
> redirects users to the second SSL site on a different port
> <https://domain.com:444>
>
> Note that if the host name in the URL is different, encryption will still
> occur successfully... the user will just get a warning box and have to
> click
> OK to continue on to the site.
>
> More info on all your IIS questions at www.iisfaq.com and
> www.iisfaq.com/ssl
>
>
>
>