From:	Alexei Roudnev
To:	Konchada, Anusha (US - Philadelphia)
Cc:	Konchada, Anusha (C); Vaswani, Ritesh (US - Mumbai); Lev Epstein; Kirill Pertsev; Deodhar, Bhushan (US - Mumbai); Ermezildo Dsouza, John (US - Mumbai); Brady, Jerry (US - Chicago); Cartee, Matthew
Subject:	Re: Action plans - Re: Understand EIS"s approach on connecting with AWS
Date:	Tuesday, October 18, 2016 10:56:14 AM

2 issues with Site-To-Site.

1) AWS uses special kind of IPSEC which has name VTI - Virtual Tunnel Interface. When used, it allows to treat IPSEC tunnel as interface, using normal routing features (static, BGP, etc routing) as we do on all routers. IT is supported by modern cisco routers only, is not supported by cisco firewalls at all, and, in many cases, can not be added where we / someone used to add IPSEC tunnels.

So it does not work as we do in normal IPSEC (which, honestly, is a huge network headache because of limitations, whioch are absent in case of VTI IPSEC) shared key, encryption, GW ip, acl lists on both sides... You instesd must establish VTI IPSEC, which creates VTI interface, and then add routing (bgp or static) as you do with any tunnel interfaces (but not with IPSEC connections).

2) IP can be incompatible with existing IP schema of the company. Then, in many cases, you/we donot want to connect AWS AAA area with main network because of security reasons.

We hit problem 1 (for problem 2, we selected IP to be compatible with both, us and CSAA, but we never checked / consider IP compatibility with own DeLoitte network). TO resolve it, we developed virtual VTI router, which we can place into DMZ we created in our private cloud, and connect with AWS (and it is simple, as this router understands AWS VTO description file). Once done, we have full connection between AWS AAA and EIS AAA networks, and we can control IN/OUT access on our firewall on EIS AAA / EIS INTRANET boundary (exactly as we do for other AAA resources). So de facto we just integrated AWS AAA network into EIS AAA network, they has full mutual access.

VTI appliance can be replaced by cisco router (new models and new IOS) or cisco virtual appliances (expensive) or some other vendors, so it is just one of the choices. But, most likely, you will need one of them, as it is unlikely that your network engineers can bring AWS VPN with VTI interfaces into your normal IPSEC infrastructure (maybe, 20% probability FOR and 80% against). We will see.

Alexei Roudnev
Senior network / data center engineer
EIS Group
Skype: Alexei_Roudnev
Cell: +1 415 806 3741

On Mon, Oct 17, 2016 at 8:56 PM, Konchada, Anusha (US - Philadelphia) <akonchada@deloitte.com> wrote:

> Hi Alexei,

Could you tell us what kind of technical issues are you referring to when you said:

But, as I said, expect technical issues with method-2, as AWS VPN is not so easy to connect from most enterprise networks.

Our primary goal is to be able to access AWS from Deloitte network without routing via EIS network and our experience on accessibility and connectivity should remain the way it was with EIS cloud.

Out of the two options you gave us- we have decided to proceed with Method#2 implementation. Now, when you say technical issues, are these issues that you might face during your implementation of method#2 or is it something that might affect the performance of our (Deloitte team's) work/ testing activities?

And, also how long do you think will it take to implement Method# 2 for us, is there any tentative timeline to establish this for us?

Thanks,

Anusha.

From: Alexei Roudnev [mailto:aroudnev@eisgroup.com]
Sent: Monday, October 17, 2016 3:33 PM
To: Konchada, Anusha (C) <Anusha.Konchada@csaa.com>
Cc: Vaswani, Ritesh (US - Mumbai) <rvaswani@DELOITTE.com>; Lev Epstein <lepstein@eisgroup.com>; Kirill Pertsev <kpertsev@eisgroup.com>; Konchada, Anusha (US - Philadelphia) <akonchada@deloitte.com>; Deodhar, Bhushan (US - Mumbai) <bdeodhar@deloitte.com>; Ermezildo Dsouza, John (US - Mumbai) <jermezildodsouza@deloitte.com>; Brady, Jerry (US - Chicago) <jebrady@deloitte.com>; Cartee, Matthew <Matthew.Cartee@csaa.com>
Subject: Re: Action plans - Re: Understand EIS's approach on connecting with AWS

Actually, method 1 and method 2 coexists in many projects. As for now, you DO USE method-1, the only change we did (in Method-1) was adding one more access point directly inside AWS so if someone connects directly to it, his traffic do not pass EIS infrastructure

> and, in some cases, he can have better response time. Or you can use old access points and they provide access to both EIS and AWS systems /to AAA development area of them/.
>
> Once you implement method 2, more and more people can work directly from your network. So eventually method 1 will be used rarely and method 2 most of the time. In some point, you can decommission method 1 (esp. if, remember, we add DeLoitte / EIS site-to-site connection too, so you can work with AWS resources and with EIS resources directly).
>
> But, as I said, expect technical issues with method-2, as AWS VPN is not so easy to connect from most enterprise networks.
>
> Alexei Roudnev
>
> Senior network / data center engineer
>
> EIS Group
>
> Skype: Alexei_Roudnev
>
> Cell: +1 415 806 3741
>
> On Mon, Oct 17, 2016 at 3:26 PM, Konchada, Anusha (C) <Anusha.Konchada@csaa.com> wrote:
>
>> Thank you, Alexei.
>>
>> Method1- Just a Prototype test which can used only for now.
>>
>> Method2 (Site- to -Site):
>>
>> I believe your comments in the below email (everything that has been highlighted) is for Site-to-Site.
>>
>> I will let the network person ask the follow up questions based on this information.
>>
>> Thanks,
>>
>> Anusha.

From: Alexei Roudnev [mailto:aroudnev@eisgroup.com]
Sent: Monday, October 17, 2016 1:31 PM
To: Konchada, Anusha (C) <Anusha.Konchada@csaa.com>
Cc: Vaswani, Ritesh (US - Mumbai) <rvaswani@deloitte.com>; Lev Epstein <lepstein@eisgroup.com>; Kirill Pertsev <kpertsev@eisgroup.com>; Konchada, Anusha (US - Philadelphia) <akonchada@deloitte.com>; Deodhar, Bhushan (US - Mumbai) <bdeodhar@deloitte.com>; Ermezildo Dsouza, John (US - Mumbai) <jermezildodsouza@deloitte.com>; Brady, Jerry <jebrady@deloitte.com>; Cartee, Matthew <Matthew.Cartee@csaa.com>
Subject: Re: Action plans - Re: Understand EIS's approach on connecting with AWS

Method 2 - comment; the method 1- what youc an use JUST NOW for the work.

See below.

METHOD 2 - site / site.

> It does not work this way with AWS. You can not establish IPSEC between your network and them, except some rare exceptions (if you have proper routers in place, can set up ACL-s and your security persons agree, have compatible IP, and so on).
>
> You need to set up some zone in your network, which will be connected with AWS. It must use IP compatible with all OUR network (not with AWS only, but with the whole EIS) and better compatible with the whole CSAA betwork (our and CSAA networks are more or less compatible on IP plans, as is AWS part of it).
>
> Then you need to set up dedicated routers, in this sandbox area (it can be HW cisco or virtual cisco or our appliance).
>
> Then we add your router as customer gateway to AWS and then set up VPN. Once setting up VPN, you generate file for your cisco or you import and parse file in our appliance; in all cases you _do not search for ipsec, key etc_ as it is all provided in a single file by AWS.
>
> And then you set up these VPN-s (it is always 2 at least) and your sandbox area became part of AWS, how to route between it and your network is, then, up to your network guys.

METHOD 1 - completed (prototype):

> I reconfigured our existing CSAA RAS servers, so you can now cionnect to our networks via any of 3 servers, using SSTP protocol:
>
> ec2-52-44-31-73.compute-1.

> > > | | | | |
> > > |---|---|---|---|
> > > | aws2aaaras01 | .eqxdev.exigengroup.com | CNAME | amazonaws.com. |
> > > | dev2aaa3ras300 | .eqxdev.exigengroup.com | A | 209.44.73.128 |
> > > | dev5aaa3ras600 | .eqxdev.exigengroup.com | A | 65.49.55.159 |
> > >
> > > First 2 allows to work with AWS only; last 2 allows to work with both EIS and AWS at the same time; authentication is the same on all 3.
> > >
> > > (
> > >
> > > Alexei Roudnev
> > >
> > > Senior network / data center engineer
> > >
> > > EIS Group
> > >
> > > Skype: Alexei_Roudnev
> > >
> > > Cell: +1 415 806 3741
> > >
> > > On Mon, Oct 17, 2016 at 8:47 AM, Vaswani, Ritesh (US - Mumbai) <rvaswani@deloitte.com> wrote:
> > >
> > > > Hi Alexei,
> > > >
> > > > Greetings for the day!!
> > > >
> > > > Thanks for setting up this prototype for us to establish VPN. However, today we've received confirmation from our management to set-up site-to-site connectivity with AWS. So, we're in a process of gathering all data(IP addresses, IKE/IPSEC Options and others). I'll let you know when we need additional inputs from your end on this set-up.
> > > >
> > > > Best Regards – Ritesh
> > > >
> > > > **Ritesh Vaswani**
> > > >
> > > > Deloitte Consulting India Pvt Ltd
> > > > U.S. Direct: +1 678 299 9895 | India Direct: +91 22 6113 9895 | VOIP: 39895
> > > >
> > > > mailto:rvaswani@deloitte.com | www.deloitte.com

Please consider the environment before printing

From: Alexei Roudnev [mailto:aroudnev@eisgroup.com]
Sent: Saturday, October 15, 2016 9:26 AM
To: Konchada, Anusha (C) <Anusha.Konchada@csaa.com>; Lev Epstein <lepstein@eisgroup.com>; Kirill Pertsev <kpertsev@eisgroup.com>
Cc: Konchada, Anusha (US - Philadelphia) <akonchada@deloitte.com>; Deodhar, Bhushan (US - Mumbai) <bdeodhar@deloitte.com>; Vaswani, Ritesh (US - Mumbai) <rvaswani@DELOITTE.com>; Ermezildo Dsouza, John (US - Mumbai) <jermezildodsouza@deloitte.com>
Subject: Re: Action plans - Re: Understand EIS's approach on connecting with AWS

Quick update:

- prototype created.

- It is much more limited in access vs when you access via our cloud RAS system, so it should be used only when someone works exclusively with AWS systems.

- it is prototype yet.

- I adjusted our SSTP servers to provide routing to both our cloud and AWS cloud,.

You can test - IT IS PROTOTYPE, I post it to save time (maybe your test reveal something important). Configure Windows VPN the same way as you do for 2 existing servers

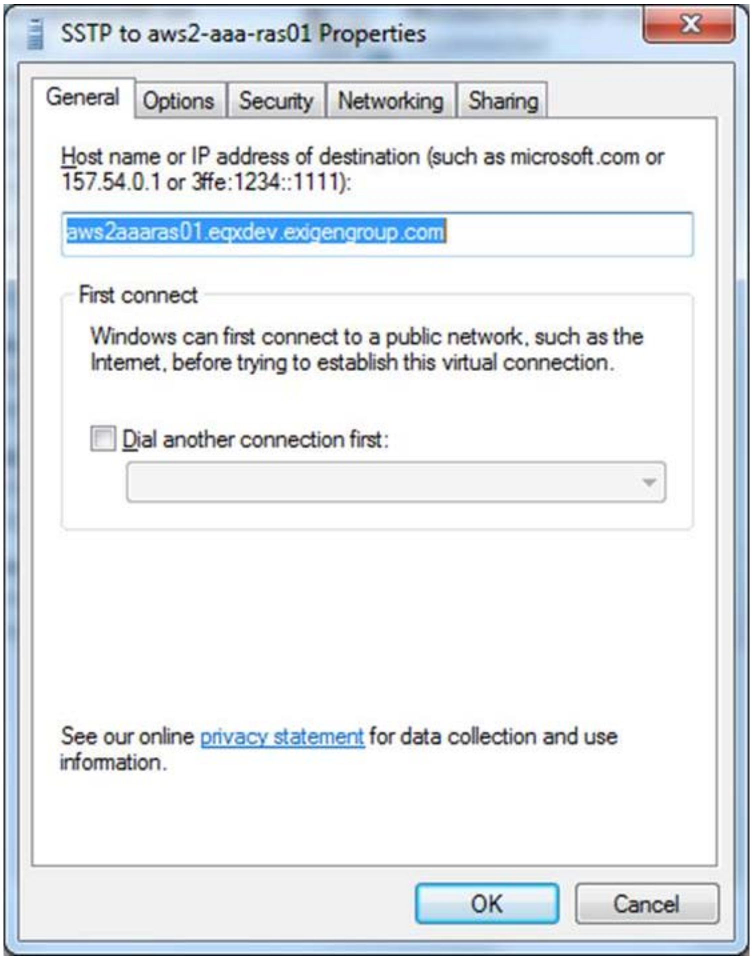
dev5aaa3ras600.eqxdev.exigengroup.com (it was down but will be back again)
dev2aaa3ras300.eqxdev.exigengroup.com

but instead use name

aws2aaaras01.eqxdev.exigengroup.com

You can TEST. IT is PROTOTYPE so it can change; detailed document will be posted shortly.

Here are screenshots (but use account which can login into our cloud) - configure new VPN as:



SSTP to aws2-aaa-ras01 Properties

Host name or IP address of destination (such as microsoft.com or 157.54.0.1 or 3ffe:1234::1111):

aws2aaaras01.eqxdev.exigengroup.com

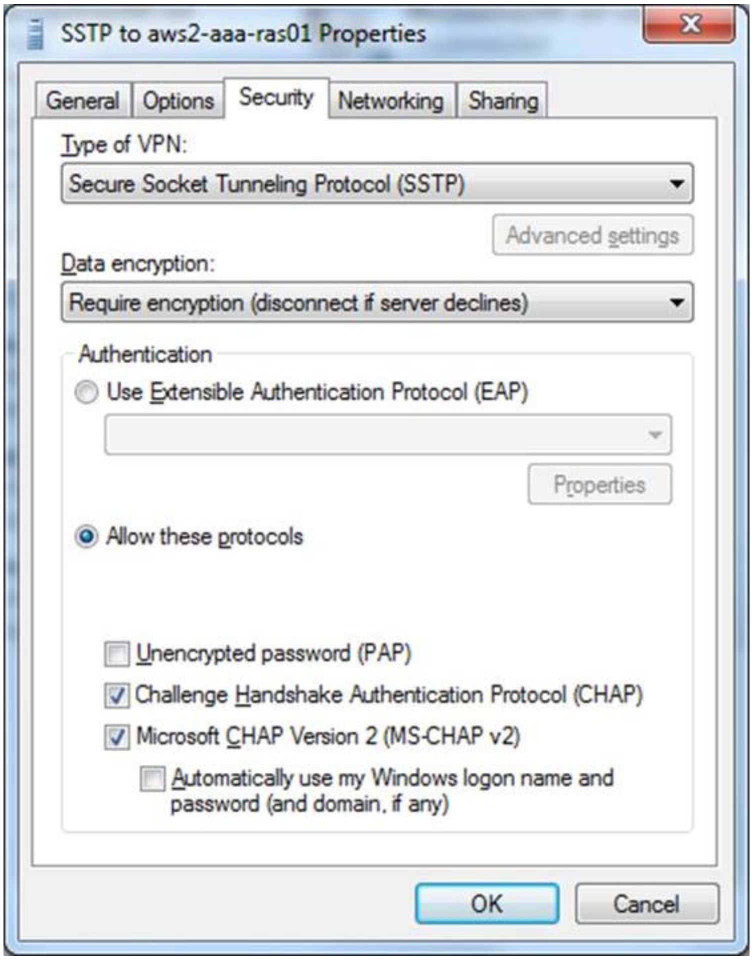
First connect

Windows can first connect to a public network, such as the Internet, before trying to establish this virtual connection.

□ Dial another connection first:

See our online privacy statement for data collection and use information.

SECURITY:



SSTP to aws2-aaa-ras01 Properties

Type of VPN:

Secure Socket Tunneling Protocol (SSTP)

Data encryption:

Require encryption (disconnect if server declines)

Authentication

○ Use Extensible Authentication Protocol (EAP)

● Allow these protocols

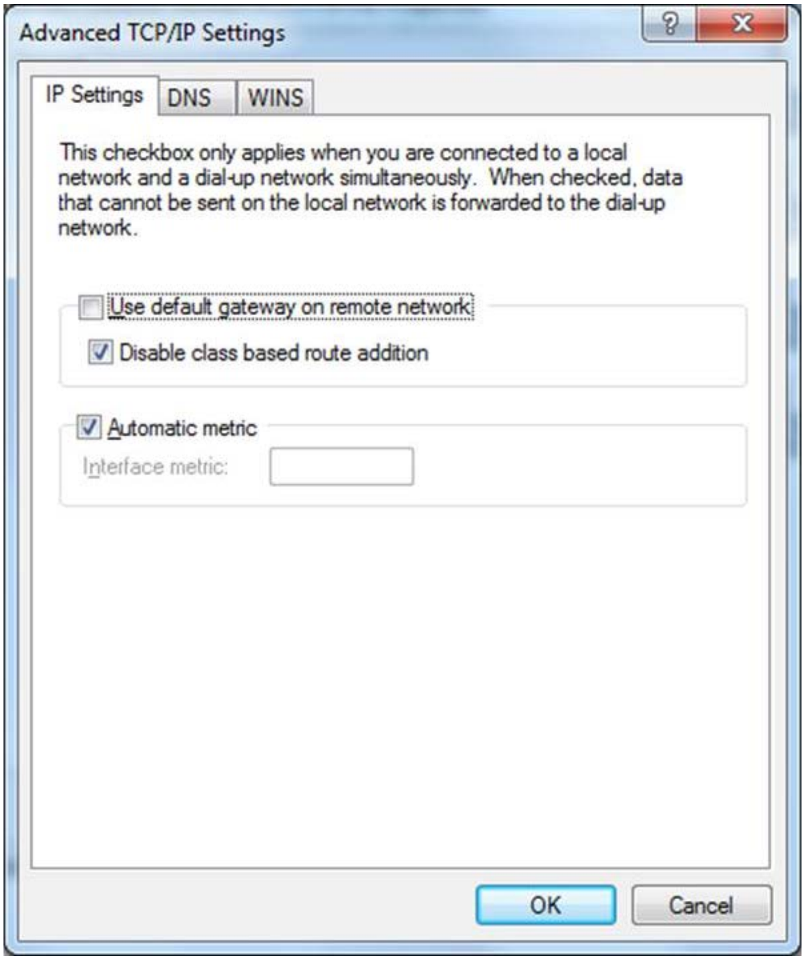
□ Unencrypted password (PAP)

☑ Challenge Handshake Authentication Protocol (CHAP)

☑ Microsoft CHAP Version 2 (MS-CHAP v2)

□ Automatically use my Windows logon name and password (and domain, if any)

Network, Properties, IPv4, ADVANCED (IMPORTANT):



This checkbox only applies when you are connected to a local network and a dial-up network simultaneously. When checked, data that cannot be sent on the local network is forwarded to the dial-up network.

□ Use default gateway on remote network

☑ Disable class based route addition

☑ Automatic metric

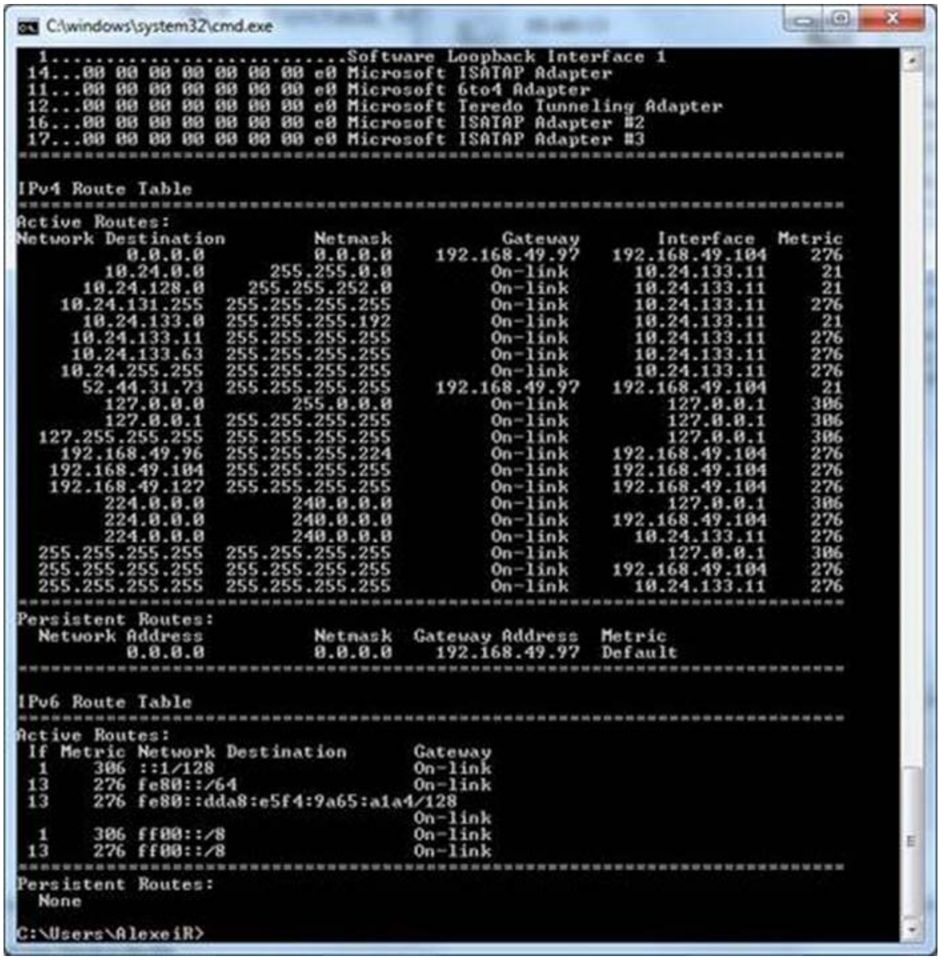
Interface metric:

Now connect with EXIGEN\<your name> (you must be in access group). if first tail fail, try again or sidable revocation verification (if fail often). Local accounts are tested (to allow login without EIS domain).

Once connected, check

```
netstat -rn
```

You must see 10.24.0.0 record



```
  1...........................Software Loopback Interface 1
 14...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
 11...00 00 00 00 00 00 00 e0 Microsoft 6to4 Adapter
 12...00 00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
 16...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
 17...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.49.97   192.168.49.104    276
        10.24.0.0      255.255.0.0         On-link       10.24.133.11     21
      10.24.128.0    255.255.252.0         On-link       10.24.133.11     21
    10.24.131.255  255.255.255.255         On-link       10.24.133.11    276
      10.24.133.0  255.255.255.192         On-link       10.24.133.11     21
     10.24.133.11  255.255.255.255         On-link       10.24.133.11    276
     10.24.133.63  255.255.255.255         On-link       10.24.133.11    276
    10.24.255.255  255.255.255.255         On-link       10.24.133.11    276
      52.44.31.73  255.255.255.255     192.168.49.97   192.168.49.104     21
        127.0.0.0        255.0.0.0         On-link          127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link          127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link          127.0.0.1    306
    192.168.49.96  255.255.255.224         On-link     192.168.49.104    276
   192.168.49.104  255.255.255.255         On-link     192.168.49.104    276
   192.168.49.127  255.255.255.255         On-link     192.168.49.104    276
        224.0.0.0        240.0.0.0         On-link          127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link     192.168.49.104    276
        224.0.0.0        240.0.0.0         On-link       10.24.133.11    276
  255.255.255.255  255.255.255.255         On-link          127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link     192.168.49.104    276
  255.255.255.255  255.255.255.255         On-link       10.24.133.11    276
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
          0.0.0.0          0.0.0.0    192.168.49.97  Default
===========================================================================

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    306 ::1/128                  On-link
 13    276 fe80::/64                On-link
 13    276 fe80::dda8:e5f4:9a65:a1a4/128
                                    On-link
  1    306 ff00::/8                 On-link
 13    276 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None

C:\Users\AlexeiR>
```

Now test

```
C:\Users\AlexeiR>ping aws2aaabld01.corevelocity.csaa.cloud.

Pinging aws2aaabld01.corevelocity.csaa.cloud [10.24.129.161] with 32 bytes of da
ta:
Reply from 10.24.129.161: bytes=32 time=86ms TTL=63
Reply from 10.24.129.161: bytes=32 time=85ms TTL=63
Reply from 10.24.129.161: bytes=32 time=84ms TTL=63
Reply from 10.24.129.161: bytes=32 time=85ms TTL=63

Ping statistics for 10.24.129.161:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 84ms, Maximum = 86ms, Average = 85ms
```

Access provided TO AWS2-AAA network ONLY (even if you can resolve names in other domains, access to them requires to be on EIS VPN, which in turn provides access to AWS too.

Alexei Roudnev

Senior network / data center engineer

EIS Group

Skype: Alexei_Roudnev

Cell: +1 415 806 3741

On Wed, Oct 12, 2016 at 9:17 AM, Konchada, Anusha (C) <Anusha.Konchada@csaa.com> wrote:

> Hi Alexei,
>
> Good morning!
>
> Thank you for sending out the detailed steps for each of the methods.
>
> Could you please confirm if we missed out listing ‘creation of DNS entries for AWS URLs within Deloitte’s domain’ as one of the steps under Method#2? Just wanted to check with you.
>
> Thanks,
>
> Anusha.
>
> **From:** Alexei Roudnev [mailto:aroudnev@eisgroup.com]
> **Sent:** Tuesday, October 11, 2016 2:30 PM
> **To:** Konchada, Anusha (US - Philadelphia) <akonchada@deloitte.com>
> **Cc:** Deodhar, Bhushan (US - Mumbai) <bdeodhar@deloitte.com>; Vaswani, Ritesh (US - Mumbai) <rvaswani@deloitte.com>; Konchada, Anusha (C) <Anusha.Konchada@csaa.com>
> **Subject:** Action plans - Re: Understand EIS's approach on connecting with AWS

method 1:

1 - open ticket and find out exact VM requirements for

(1.1) RAS server

(1.2) Proxy web server

(1.3) get approval from CSAA for these 2 instances

2 - create RAS server (WIn2K8R2 or higher), (EIS)

2.1 Create Win server and join into EXIGEN domain as for now

2.2 Assign external name with existing wildcard certificate (or request new one)

2.3 Configure SSTP and l2TP service

2.4 Configure NAT and outside access to this server.

2.5 Create local users to provide access without VPN to EIS Group

2.6 Test SSTP (EIS + customer)

2.7 Test L2TP (L2TP is created to allow access if something go wrong with SSTP SSL certificate)

3 - create WEB proxy server (EIS)

3.1 Create and configure

3.2 Assign external names as required and external wildcard certificate

3.3 Test access

Method 2 - requires private VMware or similar cloud inside DeLoitte network, or dedicated hardware (not recommended)

DeLiottte

4.1 Review architecture, get approval from network and security. Consult with EIS if necessary.

4.2 Decide on using EIS VTI appliance, commercial Cisco appliance, or hardware Cisco

4.3 Approve creating isolated sandbox inside their network, with access into it from DeLoitte, access from it to outside only, and IP compatible with all 3 companies (DeLoitte, EIS includeing AWS, and CSAA) /It is private IP/

4.4 Import VTI appliance or purchase cisco appliance or HW cisco.

4.5 Set up VTI appliance as a router with 1 port in DMZ and 1 port in OUTSIDE and default in DMZ (so no access to OUTSIDE except VTI PEERS).

4.6 Configure VPN with AWS

4.7 (optionally) configure VPN with EIS (from the same VTI router / appliance)

4.8 Configure / approve access from DeLoitte to this DMZ (optionally install virtual workstations in it).

This message (including any attachments) contains confidential information intended for a specific individual and purpose, and is protected by law. If you are not the intended recipient, you should delete this message and any disclosure, copying, or distribution of this message, or the taking of any action based on it, by you is strictly prohibited.

v.E.1