How to connect to ADFS 3.0 from NetScaler ADC load balancer?

Use Case

Use case 1: Microsoft Active Directory Federation Services (ADFS) 3.0 which provides single sign-on access to enterprise applications, requires server name in client hello extension to identify the application to connect to.

Use case 2: Connect to a server with multiple applications running on same port and indicate the application NetScaler wants to connect to, using Server Name Indication (SNI).

Introduction

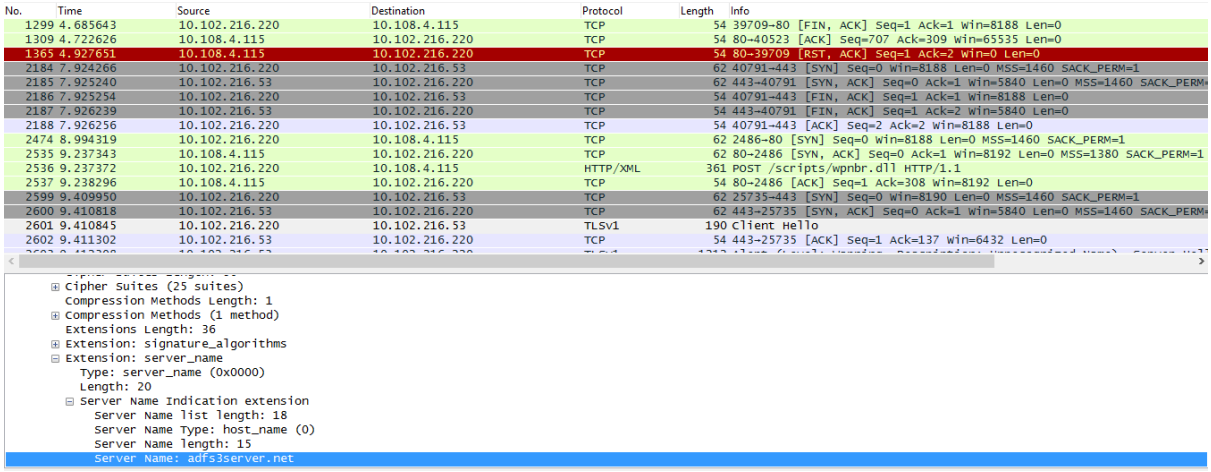
SNI has become a common feature now with most of the web browsers supporting it. Using SNI, a client informs server that which application it wants to connect to. Server then selects the SSL certificate corresponding to that application and sends it to the client. This enables a server to host multiple applications running on same IP and port and thus eases manageability.

NetScaler supports SNI on both frontend and backend connection i.e. connection from client to NetScaler and from NetScaler to server. The use cases mentioned above are related to SNI support on NetScaler backend. When SNI is configured on SSL service, NetScaler sends server name in client hello. Server is then able to decide which application to connect to sends appropriate SSL certificate to NetScaler.

Applications like Microsoft ADFS 3.0 mandates to send server name in client hello. With SNI support on backend (from 11.1 GA), NetScaler is able to connect to ADFS 3.0 as per the specification. Also, this feature allows to securely connect to any generic server hosting multiple applications on same port.

The SNI on backend support is also available on secure monitors in NetScaler. This enable NetScaler to correctly monitor applications like ADFS 3.0.

A trace taken on NetScaler captures SNIP sending server name in client hello to backend server. The server name is a static parameter of an SSL service.



No.	Time	Source	Destination	Protocol	Length	Info
1299	4.685643	10.102.216.220	10.108.4.115	TCP	54	39709→80 [FIN, ACK] Seq=1 Ack=1 Win=8188 Len=0
1309	4.722626	10.108.4.115	10.102.216.220	TCP	54	80→40523 [ACK] Seq=707 Ack=309 Win=65535 Len=0
1365	4.927651	10.108.4.115	10.102.216.220	TCP	54	80→39709 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
2184	7.924266	10.102.216.220	10.102.216.53	TCP	62	40791→443 [SYN] Seq=0 Win=8188 Len=0 MSS=1460 SACK_PERM=1
2185	7.925240	10.102.216.53	10.102.216.220	TCP	62	443→40791 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=
2186	7.925254	10.102.216.220	10.102.216.53	TCP	54	40791→443 [FIN, ACK] Seq=1 Ack=1 Win=8188 Len=0
2187	7.926239	10.102.216.53	10.102.216.220	TCP	54	443→40791 [FIN, ACK] Seq=1 Ack=2 Win=5840 Len=0
2188	7.926256	10.102.216.220	10.102.216.53	TCP	54	40791→443 [ACK] Seq=2 Ack=2 Win=8188 Len=0
2474	8.994319	10.102.216.220	10.108.4.115	TCP	62	2486→80 [SYN] Seq=0 Win=8188 Len=0 MSS=1460 SACK_PERM=1
2535	9.237343	10.108.4.115	10.102.216.220	TCP	62	80→2486 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1380 SACK_PERM=1
2536	9.237372	10.102.216.220	10.108.4.115	HTTP/XML	361	POST /scripts/wpnbr.dll HTTP/1.1
2537	9.238296	10.108.4.115	10.102.216.220	TCP	54	80→2486 [ACK] Seq=1 Ack=308 Win=8192 Len=0
2599	9.409950	10.102.216.220	10.102.216.53	TCP	62	25735→443 [SYN] Seq=0 Win=8190 Len=0 MSS=1460 SACK_PERM=1
2600	9.410818	10.102.216.53	10.102.216.220	TCP	62	443→25735 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=
2601	9.410845	10.102.216.220	10.102.216.53	TLSv1	190	Client Hello
2602	9.411302	10.102.216.53	10.102.216.220	TCP	54	443→25735 [ACK] Seq=1 Ack=137 Win=6432 Len=0

```
⊞ Cipher Suites (25 suites)
  Compression Methods Length: 1
⊞ Compression Methods (1 method)
  Extensions Length: 36
⊞ Extension: signature_algorithms
⊟ Extension: server_name
    Type: server_name (0x0000)
    Length: 20
  ⊟ Server Name Indication extension
      Server Name list length: 18
      Server Name Type: host_name (0)
      Server Name length: 15
      Server Name: adfs3server.net
```

Configuration Steps in NetScaler ADC

CLI:

> add service <service name> <service IP> SSL 443

> set ssl service <service name> -SNIEnable ENABLED –commonName adfs3server.net

For more information please see the official documentation site –

http://docs.citrix.com/en-us/netscaler/11-1/ssl/config-ssloffloading/support_for_sni_on_backend_service.html