ADAPTURE
THINK FORWARD.

White Paper

Supporting SHA1 and SHA2 in the Same Virtual Server Using F5 Networks Local Traffic Manager

WRITTEN BY:

Tim Cullen, CISSP, F5-CTS // Rob Lluis, Aptive Solutions, Inc. //
Russ Via // Jacob Hunt // Cedric Caldwell

Contents

Tim Cullen, CISSP, F5-CTS

Tim Cullen is a Certified Information Security Systems Professional (CISSP) at ADAPTURE specializing in information security and network architecture. Tim has participated in and organized security events, talks, training, and new product testing and integration for over 25 years. He has helped develop corporate security strategies and assessments throughout his security career.

Document Objective

This document is to explain the design behind the support for SHA1 and SHA2 within the same virtual server using F5 Networks' Local Traffic Manager, and illustrate the steps necessary for creating this environment.

Design Considerations

The customer's environment had a mixture of SSLv3 and TLS Point-of-Sale devices. The devices were not able to have the encryption level upgraded or changed and unmanned. This caused a unique issue with the POS terminals. Since they were unmanned with no ability to renegotiate on their own, if there were any disruption in the SSL communication, the transaction would fail, and that would mean lost revenue. A final condition was that the communications were not HTTP based. The communications needed to be encrypted on multiple non-standard ports.

Customer Environment and Limitations

First, let's discuss the different levels and their limitations with respect to Data Integrity

- Thousands of "Point-of-Sale" machines deployed all over the world
- No ability to upgrade the supported encryption level on many of the devices
- SSLv3/SHA1 Certificates expired soon with no ability to renew them at the same level
- Only one SSL inspection allowed
- Not using HTTP protocol, 15 different non-standard ports
- SSLv3 is necessary as well as support for TLS all versions
- Some POS terminals could only negotiate at SSLv3

Solution Design

The solution had to allow for access to all of the 15 separate virtual servers and custom ports while being able to selectively authenticate the client certificates at the highest level of encryption that the device could.

SSL negotiations, by default, will negotiate at the best possible encryption available as dictated by the client. In this case, however, the limitation was in the compatibility matrix of the encryption levels.

First, let's discuss the different levels and their limitations with respect to Data Integrity.

Algorithm	SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3 (Draft)	Status
HMAC-MD5	Yes	Yes	Yes	Yes	Yes		Defined for TLS 1.2 in RFCs
HMAC-SHA1	No	Yes	Yes	Yes	Yes		
HMAC-SHA256/384	No	No	No	No	Yes		
AEAD	No	No	No	No	Yes		
GOST 28147-89 IMIT	No	No	Yes	Yes	Yes		Proposed in RFC drafts
GOST R 34.11-94	No	No	Yes	Yes	Yes		

As you can see from the list, HMAC-SHA1 supports versions SSLv3 to TLS1.2. The HMAC-SHA256/384 supports TLS1.2 only. This means that if a device only supported SSLv3, it would not be able to negotiate a SHA2x level negotiation and would fail. All SHA2 connections would only be able to connect at SHA1, and the encryption and cipher would be downgraded as well to a lower level to support the available ciphers. If we tried to set the SSL level to SHA2 only, all SSLv3 devices will fail due to the incompatibility between SHA2 and SSLv3.

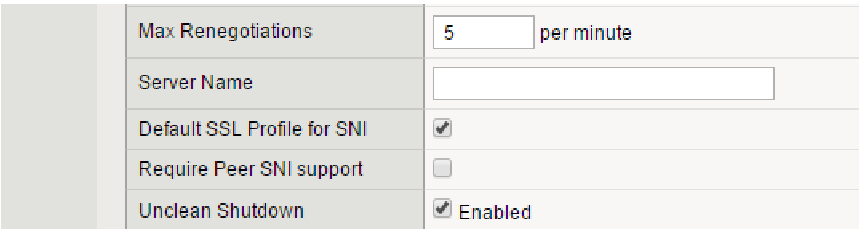
That left us with a SHA1 level negotiation as the only level of client negotiations that could be used. All other connections, regardless of the encryption level or capability, would demote their negotiation to SHA1. Since this is an insecure practice, and no longer supported by browsers or secure sites, we needed to a create a configuration that would give us the flexibility to support the SHA1 connection requests while still allowing SHA2 connections to connect at their TLS level and utilize the SHA2 hash. The overall end goal was to move to SHA2 only and support SHA1 during the migration period in a way that would not affect the customer experience, while allowing seamless transition during the migration process.

One final piece to deal with was the certificate expiration for the SHA1 certificates. This issue created a situation that required a unique certificate solution approach. This could not be handled by technology alone.

Solution Architecture

Using F5 Networks Local Traffic Manager, we were able to create two specific SSL profiles; one for SHA1 SSL, and one for SHA2 SSL level certificates.

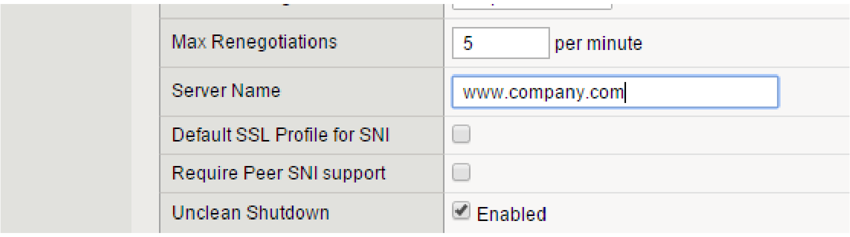
On the SHA1 Client SSL Profile, we set the option for **"Default SNI"**



Max Renegotiations	5 per minute
Server Name	
Default SSL Profile for SNI	☑
Require Peer SNI support	☐
Unclean Shutdown	☑ Enabled

SHA1 SNI SETTINGS

On the SHA2 Client SSL, we entered the **"Server Name"** of the certificate's FQDN

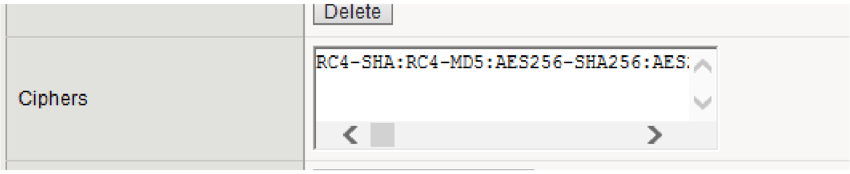


Max Renegotiations	5 per minute
Server Name	www.company.com
Default SSL Profile for SNI	☐
Require Peer SNI support	☐
Unclean Shutdown	☑ Enabled

SHA2 SNI SETTINGS

We created a custom cipher string for the profiles to allow support of SSLv3 on both profiles. The profiles had DEFAULT in as a standard, but that dropped support for SSLv3 which we needed for this deployment. The custom cipher string used in this design was:

RC4-SHA:RC4-MD5:AES256-SHA256:AES256-SHA:ECDHE-RSA-AES256-CBC-SHA:DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:AES256-SHA:DES-CBC3-SHA:ECDHE-RSA-DES-CBC3-SHA:DHE-RSA-DES-CBC3-SHA:DES-CBC3-SHA:AES128-SHA256:AES128-SHA:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES128-CBC-SHA:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA:AES128-SHA:SSLv3:MD5+TLSv1:!ADH:!EXPORT40:!EXP:!LOW

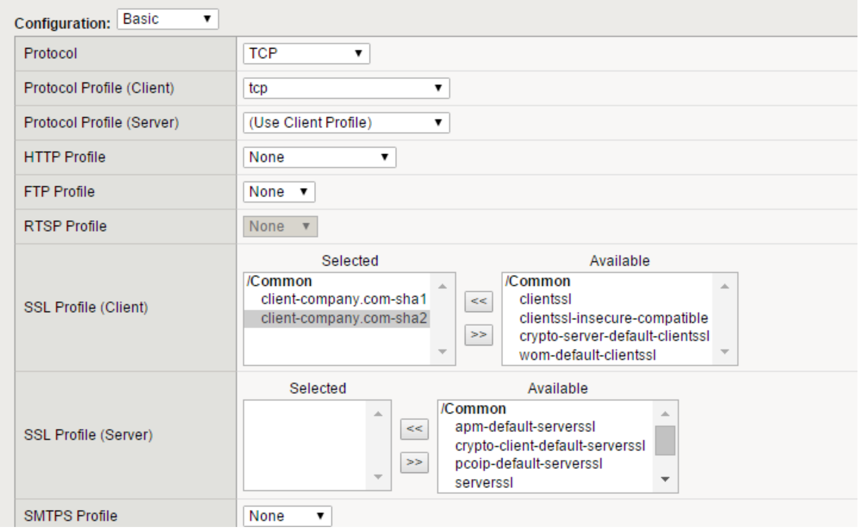


Ciphers	RC4-SHA:RC4-MD5:AES256-SHA256:AES:

CIPHER LIST

Both Client SSL profiles needed to have the same cipher string, or they would not be able to be added to the same virtual server. If you tried to save the virtual server settings, it would error out if they were different. This is the only thing that is required when using multiple certificates on one virtual server.

Once the profiles were configured, we installed them both on to the virtual server in the Client SSL profile settings.



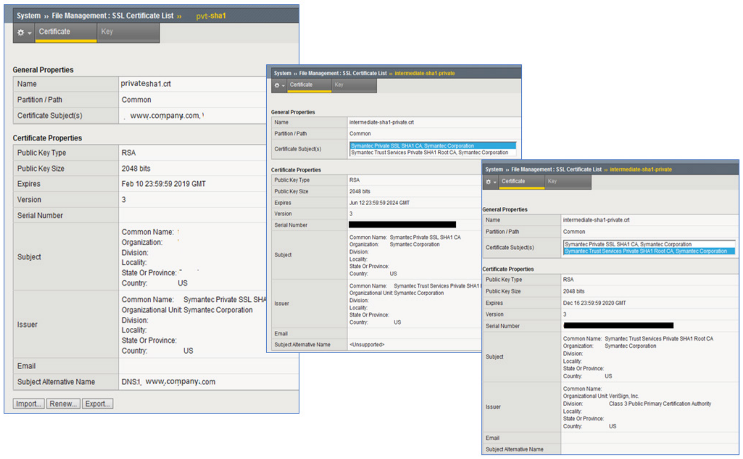
Configuration: Basic

Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile	None
FTP Profile	None
RTSP Profile	None
SSL Profile (Client)	Selected: /Common client-company.com-sha1 client-company.com-sha2 Available: /Common clientssl clientssl-insecure-compatible crypto-server-default-clientssl wom-default-clientssl
SSL Profile (Server)	Selected: Available: /Common apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl serverssl
SMTPS Profile	None

CLIENT SSL
STACKED CERTS

Extendibility of SHA1 Support

The final task was to create support for the expiring SHA1 certificates. We created a Private SHA1 certificate from the root Certificate Authority and used the same SHA1 Intermediate CA for binding the certificate. This created a Private SSLv3 SHA1 certificate with a valid Intermediate CA. This worked without presenting an SSL error or warning during communication, and the terminals were able to communicate as needed.



System » File Management : SSL Certificate List » pvt-sha1

General Properties

Name	privatesha1.crt
Partition / Path	Common
Certificate Subject(s)	www.company.com,

Certificate Properties

Public Key Type	RSA
Public Key Size	2048 bits
Expires	Feb 10 23:59:59 2019 GMT
Version	3
Serial Number	
Subject	Common Name: Organization: Division: Locality: State Or Province: Country: US
Issuer	Common Name: Symantec Private SSL SHA Organizational Unit: Symantec Corporation Division: Locality: State Or Province: Country: US
Email	
Subject Alternative Name	DNS:, www.company.com

System » File Management : SSL Certificate List » intermediate-sha1-private

General Properties

Name	intermediate-sha1-private.crt
Partition / Path	Common
Certificate Subject(s)	Symantec Private SSL SHA1 CA, Symantec Corporation Symantec Trust Services Private SHA1 Root CA, Symantec Corporation

Certificate Properties

Public Key Type	RSA
Public Key Size	2048 bits
Expires	Jun 12 23:59:59 2024 GMT
Version	3
Serial Number	[redacted]
Subject	Common Name: Symantec Private SSL SHA1 CA Organization: Symantec Corporation Division: Locality: State Or Province: Country: US
Issuer	Common Name: Symantec Trust Services Private SHA1 Organizational Unit: Symantec Corporation Division: Locality: State Or Province: Country: US
Email	
Subject Alternative Name	<Unsupported>

System » File Management : SSL Certificate List » intermediate-sha1-private

General Properties

Name	intermediate-sha1-private.crt
Partition / Path	Common
Certificate Subject(s)	Symantec Private SSL SHA1 CA, Symantec Corporation Symantec Trust Services Private SHA1 Root CA, Symantec Corporation

Certificate Properties

Public Key Type	RSA
Public Key Size	2048 bits
Expires	Dec 16 23:59:59 2020 GMT
Version	3
Serial Number	[redacted]
Subject	Common Name: Symantec Trust Services Private SHA1 Root CA Organization: Symantec Corporation Division: Locality: State Or Province: Country: US
Issuer	Common Name: Organizational Unit: VeriSign, Inc. Division: Class 3 Public Primary Certification Authority Locality: State Or Province: Country: US
Email	
Subject Alternative Name	

PRIVATE CERT AND INTERMEDIATE CA

Conclusion

The entire configuration was contained within profiles and standard virtual server options, and no iRules were needed. This created an easily supportable solution for when the F5 appliances were upgraded, as there were no custom scripts or manual iRules that needed support.

There are some things that are worth mentioning about this design. Creating support for SHA1 will help get through the immediate issue of expired and deprecated certificates, but it leaves in place one problem. The problem is that the design allows an insecure communication path into the corporate environment. While this configuration allows some breathing room from the impending deadline, it should in no way be the final solution. This design is only to be used to help give the organization some flexibility when having to replace certificates or devices. This should be used as a roadmap to phase out SHA1 certificates in a time/cost effective manner, but not as a long-term solution.

Reclaim efficiency and security in your F5 environment with access to F5 expertise when you need it most.

Contact us to learn more about F5 Managed Services.