SSL-TLS VPN

Certification Testing Report

Fortinet, Inc.
FortiGate Consolidated Security Platforms

Tested against this standard
ICSA Labs Network SSL-TLS VPN Criteria Version 4.0

August 24, 2020

Prepared by ICSA Labs
1000 Bent Creek Blvd., Suite 200
Mechanicsburg, PA 17050
www.icsalabs.com

ICSA Labs SSL-TLS VPN
Certification Testing Report

FORTINET

FortiGate Consolidated Security Platforms

https://www.fortinet.com/products/vpn.html

Model Tested: Model 501E

Firmware: V6.2.2 build 1010 (GA)

ICSA labs CERTIFIED SSL VPN

Certified
Since December 2008

Summary of Test Results

Protocol and Cipher Suite Support	TLS version tested: TLS_1.2	
	Cipher suite tested: TLS_RSA_WITH_AES_256_GHCM_SHA386	
X.509 Certificate Management and Validation	Proper certificate management with external CA	✓
	Supports client certificate authentication and proper validation	✓
	Standalone Client server certificate validation	✓
Security Testing	No unauthorized administrative access	✓
	No remote vulnerabilities found	✓
	Properly enforces security policies	✓
	Not susceptible to DoS attacks	✓
Administration	Secure remote administrative access	✓
Logging	Robust logging of security related events	✓
SSL VPN Client Platforms	Windows 10	
Authentication and Authorization	Two-factor authentication	✓
	External AAA server support	✓
	Access control	✓
	Client host integrity checks	✓
Session Control	Automatic and administrative session termination	✓
Functional Testing	L3VP	✓

About ICSA Labs

The goal of ICSA Labs is to significantly increase user and enterprise trust in information security products and solutions by establishing publicly vetted requirements and developing robust test methodologies. For nearly thirty years, ICSA Labs has performed independent, third-party security certification testing of computer and network security products, beginning with anti-malware testing in 1991.

SSL-TLS VPN Certification Testing

ICSA Labs began testing SSL-TLS VPN solutions in 2004 based on criteria developed by a consortium of SSL-TLS VPN vendors with input from industry analysts and the end user community. Since then, the focus of ICSA Labs SSL-TLS VPN testing is verifying support for enterprise level SSL-TLS VPN functionality.

More specifically, ICSA Labs SSL-TLS VPN testing confirms that tested products properly implement TLS with strong cipher suite support, while providing certificate management and validation. Additionally, testing includes proper authentication and authorization, session control and secure operation in either a Reverse Web Proxy or Layer 3 VPN mode.

Also tested are platform security of the product itself, logging, secure administration, and administrative functions.

> "…ICSA Labs SSL-TLS VPN testing confirms that tested products properly implement TLS with strong cipher suite support, while providing certificate management and validation."

Certified Product Details

Fortinet provided the hardware, software, administrative documentation and any necessary licenses to perform testing. The model, software and versions listed below successfully met all mandatory requirements.

- **FortiGate 501E (FortiOS version 6.2.2 Build 1010(GA))**
- **FortiClient (version 6.0.9.0277)**

ICSA Labs SSL-TLS VPN Certification extends beyond the most recently tested model to the other members of the FortiGate Consolidated Security Platforms. In the case of a certified family of models like that of Fortinet, ICSA Labs periodically tests other models in the series in addition to the one tested during the most recent test cycle.

FortiGate/ FortiWifi 30E	FortiGate 40F	FortiGate/FortiWifi 51E	FortiGate 60F	FortiGate/FortiWifi 61E
FortiGate 81E/FortiWifi 81E-POE	FortiGate/FortiWifi 91E	FortiGate 100E/101E	FortiGate 100F/101F	FortiGate 200E/201E
FortiGate 300D	FortiGate 300E/301E	FortiGate 400E/401E	FortiGate 500E/501E	FortiGate 600D
FortiGate 600E/601E	FortiGate 800D	FortiGate 1000D	FortiGate 1100E/1101E	FortiGate 1200D
FortiGate 1500D	FortiGate 2000E	FortiGate 2200E/2201E	FortiGate 2500E	FortiGate 3000D
FortiGate 3300E/3301E	FortiGate 3700D	FortiGate 3800D	FortiGate 3960E	FortiGate 3980E
FortiGate 5000	FortiGate 6300E/6301E	FortiGate 6500E/6501E	FortiGate 7030E	FortiGate 7040E
FortiGate 7060E				

Scope of Assessment

ICSA Labs tests candidate SSL-TLS VPN products against publicly available criteria initially developed by a consortium of SSL-TLS VPN vendors with input from industry analysts and the end user community. An ICSA Labs certified SSL-TLS VPN product must satisfy all the mandatory requirements along with all related requirements to elected optional functionality. For more information about the criteria, please visit the SSL-TLS section of the ICSA Labs website (www.icsalabs.com).

The following is a summary of the SSL-TLS VPN requirements:

1. **Protocol and Cipher Suite Support** – The TLS protocol and underlying cryptography must be implemented properly.
2. **X.509 Certificate Management and Validation** – The product must support X.509 certificate management such as secure enrollment and renewal. When supporting client certificate authentication, the product must properly validate client certificates. SSL VPN Client apps must support proper certificate validation for SSL VPN Server certificates.
3. **Security Testing** – The product must prevent unauthorized access and protect against common exploits and attacks.
4. **Administration** – The product must have secure administrative capabilities including strong authentication, secure remote access, and administrative and user session management.
5. **Logging** – The product must have the ability to accurately log the required data for system and session related events.
6. **SSL VPN Client Platforms** – The product must support a Windows based client with Internet Explorer or Firefox for browser based access.
7. **Authentication and Authorization** – The product must support secure user authentication mechanisms, including strong authentication and granular control of access to resources. The product must also have the ability to perform integrity checks of the client system before granting access and throughout the session.
8. **Session Control** – The product must provide automatic controls of user sessions.
9. **Functional Testing** – The product must support at least one mode of operation, Reverse Web Proxy (RWP) or Layer 3 VPN (L3VPN). Only the mode(s) that meet all related requirements will be documented in this report. When operating in RWP mode, the product must prevent leaking of internal network information and properly clean session related data. Typically, this requirement is satisfied with the use of a cache cleaning mechanism or a virtual desktop environment during the VPN session. In a L3VPN operation, the product must support proper disabling of split tunneling and prevent bypassing the VPN tunnel.

Testing Details

General Notes

Installation began by following the information in the included manual, ***"The FortiOS – Cookbook Version 6.2.2"*** and then referring to the Fortinet Support site (support.fortinet.com).

Protocol and Cipher Suite Support

No additional configuration was required to enable strong ciphers. The FortiClient connected to the FortiGate 501E using TLS version 1.2 and with the following cipher suite:

```
TLS_RSA_WITH_AES_256_GHCM_SHA386.
```

X.509 Certificate Management and Validation

Certificate generation and management is controlled via the GUI under the "System" menu and the "Certificates" submenu. In the "Certificates" submenu you can create certificate signing requests for certificates to be signed by an external CA. Attempts to import improper certs such as those which are expired, or improperly signed were not accepted by the appliance.

The FortiClient was also able to detect an improper certificate chain as well as improperly signed certificates. When either of these occurred, the user is notified with a pop up message.

Security Testing

After performing various tests to detect for known vulnerabilities it was determined the FortiGate 501E was not vulnerable to known exploits. The FortiGate 501E was also subjected to DoS attacks during which there was no appreciable performance degradation.

Administration

The FortiGate 501E supports secure remote administration via HTTPS and SSH. By default administrative users can reach the administrative interface on HTTP which redirects to HTTPS. HTTP can be disabled entirely on a per interface basis in the GUI under "Network Interfaces." The following CLI commands were issued to prevent insecure management connections over HTTP.

```
#config system global
(global#set admin-https-ssl-versions tls 1-2
```

Logging

All logging requirements were verified using an external syslog server. Remote logging is configured by navigating to "Log & Report" -> "Log Settings". Within that area, toggle on "Send logs to syslog" and fill in "IP Address/FQDN". Initially expired CRL messages were logged with "reason = No matching CA", Fortinet provided patch version 6.2.0 Build 1010 (Interim) which modified the expired CRL log message to reflect what is shown in the second example log message below.

Example log data from an administrator-initiated reboot:

```
Jun 23 11:19:51 <23.2> 198.18.102.1 date=2020-06-22 time=12:19:38
devname="Fortigate_SSL_VPN_Test" devid="FG5H1E5818904385" logid="0100032138"
type="event" subtype="system" level="critical" vd="root"
eventtime=1592842778281090667 tz="-0400" logdesc="Device rebooted"
user="admin" ui="GUI(172.26.25.234)" action="reboot" msg="User admin rebooted
the device from GUI(172.26.25.234). The reason is 'restarting appliance'"
```

Example log data following an expired CRL rejected by the appliance:

```
Aug 11 13:36:24 <23.6> 198.18.102.1 date=2020-08-10 time=14:35:55
devname="Fortigate_SSL_VPN_Test" devid="FG5H1E5818904385" logid="0101041990"
type="event" subtype="vpn" level="information" vd="root"
eventtime=1597084556165444064 tz="-0400" logdesc="Certificate update failed"
action="alert" cert-type="CRL" status="failure" name="CRL_2" method="HTTP"
reason="Uploaded CRL expired" msg="Certificate update failed"
```

SSL VPN Client Platforms

The client system used was Microsoft Windows 10 Pro Version 10.0.18362 Build18362 with FortiClient Version 6.0.9.0277. Internet Explorer 11 was used primarily as the web browser. Note that an administrative user account on the Windows 10 system was used to install the FortiClient.

Authentication and Authorization

ICSA Labs configured SSL VPN client access to use two-factor authentication with client certificates. ICSA Labs made several attempts to bypass proper authentication but none of these attempts were successful. Configuration for client certificate authentication is documented in ***"The FortiOS – Cookbook Version 6.2.2"***. ICSA Labs edited the policy to check that the username entered by the user in the FortiClient matched something within the client certificate Subject Name field (e.g. Common Name).

ICSA Labs verified the FortiGate's client-side integrity checking capability. The following checks were enabled for the client system at session establishment:

- firewall enabled and the version;
- AV enabled and the version;
- the OS and build version.

Client integrity checking was configured using the following commands on the windows client to gather version information about AV and Firewall products. From a Windows Power Shell prompt, the following commands were run to determine the executable path and instance GUID of the active Firewall and AV product.

```
gwmi -Namespace ROOT\securitycenter2 -Class antivirusproduct
gwmi -Namespace ROOT\securitycenter2 -Class firewallproduct
```

The result of running the former is captured in the image below. The GUID and path are highlighted

```
PS C:\Users\wayne> gwmi -Namespace root/securitycenter2 -Class AntivirusProduct


__GENUS                 : 2
__CLASS                 : AntiVirusProduct
__SUPERCLASS            :
__DYNASTY               : AntiVirusProduct
__RELPATH               : AntiVirusProduct.instanceGuid="{D68DDC3A-831F-4fae-9E44-DA132C1ACF46}"
__PROPERTY_COUNT        : 6
__DERIVATION            : {}
__SERVER                : VWIN10-1
__NAMESPACE             : ROOT\securitycenter2
__PATH                  : \\VWIN10-1\ROOT\securitycenter2:AntiVirusProduct.instanceGuid="{D68DDC3A-831F-4fae-9E44-DA132C1ACF46}"
displayName             : Windows Defender
instanceGuid            : {D68DDC3A-831F-4fae-9E44-DA132C1ACF46}
pathToSignedProductExe  : windowsdefender://
pathToSignedReportingExe : %ProgramFiles%\Windows Defender\MsMpeng.exe
productState            : 393472
timestamp               : Mon, 17 Aug 2020 18:58:56 GMT
PSComputerName          : VWIN10-1

__GENUS                 : 2
__CLASS                 : AntiVirusProduct
__SUPERCLASS            :
__DYNASTY               : AntiVirusProduct
__RELPATH               : AntiVirusProduct.instanceGuid="{18A975F9-A60C-37D8-E30B-4BEF31AD3411}"
__PROPERTY_COUNT        : 6
__DERIVATION            : {}
__SERVER                : VWIN10-1
__NAMESPACE             : ROOT\securitycenter2
__PATH                  : \\VWIN10-1\ROOT\securitycenter2:AntiVirusProduct.instanceGuid="{18A975F9-A60C-37D8-E30B-4BEF31AD3411}"
displayName             : AVG Antivirus
instanceGuid            : {18A975F9-A60C-37D8-E30B-4BEF31AD3411}
pathToSignedProductExe  : C:\Program Files\AVG\Antivirus\wsc_proxy.exe
pathToSignedReportingExe : C:\Program Files\AVG\Antivirus\wsc_proxy.exe
productState            : 266240
timestamp               : Mon, 17 Aug 2020 18:57:52 GMT
PSComputerName          : VWIN10-1
```

Once the executable path of the AV or Firewall product is returned, run the command below to determine the version number. Highlighted below in the image is the version number of the AV product.

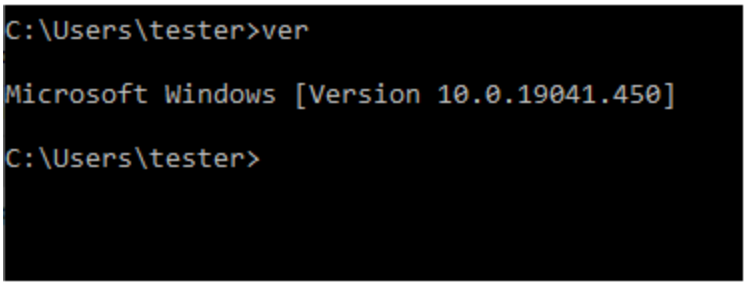
```
Get-item '<path to signed executable from previous command>' |Format-list
```

```
PS C:\Users\wayne> get-item 'C:\Program Files\AVG\Antivirus\wsc_proxy.exe'|Format-list


    Directory: C:\Program Files\AVG\Antivirus


Name           : wsc_proxy.exe
Length         : 110608
CreationTime   : 8/17/2020 2:56:15 PM
LastWriteTime  : 8/17/2020 2:56:15 PM
LastAccessTime : 8/17/2020 3:14:27 PM
Mode           : -a----
LinkType       :
Target         : {}
VersionInfo    : File:             C:\Program Files\AVG\Antivirus\wsc_proxy.exe
                 InternalName:     wsc_proxy
                 OriginalFilename: wsc_proxy.exe
                 FileVersion:      20.6.5495.0
                 FileDescription:  AVG remediation exe
                 Product:          AVG Internet Security System
                 ProductVersion:   20.6.5495.0
                 Debug:            False
                 Patched:          False
                 PreRelease:       False
                 PrivateBuild:     False
                 SpecialBuild:     False
```

Once the information is collected from PowerShell, the following CLI configuration changes were made on the FortiGate appliance:

```
#conf vpn ssl web host-check-software
#edit <provide a policy name, e.g., "Custom AVG AV">
#set type <enter "FW" or "AV">
#set guid <use the GUID output from the power shell script>
#set version < use the version number output from the power shell script >
#end
#conf vpn ssl web portal
#edit <provide the portal name in use>
#set host-check custom
#set host-check-policy <provide same policy name as above>
#end
```

To inspect hosts for a specific version of Microsoft Windows run the "ver" command from a windows CLI prompt as shown in the image below.



Using the information returned after issuing the ver command in the image above, the following configuration details were added to the FortiGate device.

```
#config vpn ssl web portal
(portal)#edit <provide your VPN portal name>
(VPN portal name)#set os-check enable
(VPN portal name)set config os-check-list windows-10
(windows-10)#set action check-up-to-date
(windows-10)#set tolerance 0
(windows-10)# set latest-patch level 19041
(windows-10)#end
(VPN portal name)#end
```

Session Control

Since testing was performed using the FortiClient rather than a web browser, session timeout was controlled via schedule re-authentication timeout. To configure the re-authentication timeout, administrators can use the following commands from the CLI:

```
#config vpn ssl settings
#set auth-timeout (timeout in seconds)
#end
```

Functional Testing

During testing, ICSA Labs disabled split tunneling. Disabling split tunneling forces all client traffic to pass through the VPN. With split tunneling disabled, ICSA Labs attempted to pass traffic outside the VPN. To do so, ICSA Labs configured a more specific route in the Windows routing table than originally added by the FortiClient. The FortiClient then lowered the metric of the VPN route to take precedence over the route added during testing. ICSA Labs also attempted to delete the VPN route, these attempts were unsuccessful. Ultimately, ICSA Labs was unable to disrupt routing from the client while split tunneling was disabled.

Authority

This report is issued by the authority of the General Manager, ICSA Labs. Tests are performed under normal operating conditions.

Sebastien Mazas, General Manager, ICSA Labs

ICSA Labs

The goal of ICSA Labs is to significantly increase user and enterprise trust in information security products and solutions. For nearly 30 years, ICSA Labs, an independent division of Verizon, has been providing credible, independent, 3rd party security product testing and certification for many of the world's top security product developers and service providers. Enterprises worldwide rely on ICSA Labs to set and apply objective testing and certification criteria for measuring product compliance and performance.

www.icsalabs.com

Fortinet, Inc.

Fortinet's mission is to deliver the most innovative, highest performing network security platform to secure and simplify your IT infrastructure. We are a leading global provider of network security appliances for carriers, data centers, enterprises and distributed offices. Because of our custom ASICs, hardware systems, network software, management capabilities and security research, we have a large, rapidly growing customer base, including the majority of the Fortune Global 100. Our market position and solution effectiveness has been widely validated by industry analysts, independent testing labs, business organizations, and the media worldwide. Our broad product line of complementary solutions goes beyond Network Security to help secure the extended enterprise.

www.fortinet.com