FQDN Support for IPsec

Application Note

201106-01
Rev 1.1

Important Notice

Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors) or be totally lost. Although significant delays or losses of data are rare when wireless devices such as the Sierra Wireless AirLink modem are used in a normal manner with a well-constructed network, the Sierra Wireless AirLink modem should not be used in situations where failure to transmit or receive data could result in personal hazard or risk to the user or any other party, including but not limited to personal injury, death, or loss of property. Sierra Wireless accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the Sierra Wireless AirLink modem, or for failure of the Sierra Wireless AirLink modem to transmit or receive such data.

Safety and Hazards

Do not operate the Sierra Wireless AirLink modem in areas where blasting is in progress, near medical equipment, near life support equipment, or near any equipment which may be susceptible to any form of radio interference. In such areas, the Sierra Wireless AirLink modem **MUST BE POWERED OFF**. The Sierra Wireless AirLink modem can transmit signals that could interfere with this equipment.

Do not operate the Sierra Wireless AirLink modem in any aircraft, whether the aircraft is on the ground or in flight. In aircraft, the Sierra Wireless AirLink modem **MUST BE POWERED OFF**. When operating, the Sierra Wireless AirLink modem can transmit signals that could interfere with various onboard systems.

Note: Some airlines may permit the use of cellular phones while the aircraft is on the ground and the door is open. Sierra Wireless AirLink modem may be used at this time.

The driver or operator of any vehicle should not operate the Sierra Wireless AirLink modem while in control of a vehicle. Doing so will detract from the driver or operator's control and operation of that vehicle. In some states and provinces, operating such communications devices while in control of a vehicle is an offense.

Limitation of Liability

The information in this manual is subject to change without notice and does not represent a commitment on the part of Sierra Wireless. SIERRA WIRELESS AND ITS AFFILIATES SPECIFICALLY DISCLAIM LIABILITY FOR ANY AND ALL DIRECT, INDIRECT, SPECIAL, GENERAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR REVENUE OR ANTICIPATED PROFITS OR REVENUE ARISING OUT OF THE USE OR INABILITY TO USE ANY SIERRA WIRELESS PRODUCT, EVEN IF SIERRA WIRELESS AND/OR ITS AFFILIATES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR THEY ARE FORESEEABLE OR FOR CLAIMS BY ANY THIRD PARTY.

Notwithstanding the foregoing, in no event shall Sierra Wireless and/or its affiliates aggregate liability arising under or in connection with the Sierra Wireless product, regardless of the number of events, occurrences, or claims giving rise to liability, be in excess of the price paid by the purchaser for the Sierra Wireless product.

Patents

This product includes technology licensed from QUALCOMM® 3G.

Manufactured or sold by Sierra Wireless Inc. or its licensees under one or more patents licensed from InterDigital Group.

Copyright

Trademarks

AirCard® and Watcher® are registered trademarks of Sierra Wireless. Sierra Wireless™, AirPrime™, AirLink™, AirVantage™ and the Sierra Wireless logo are trademarks of Sierra Wireless.

Windows® and Windows Vista® are registered trademarks of Microsoft Corporation.

Macintosh and Mac OS X are registered trademarks of Apple Inc., registered in the U.S. and other countries.

QUALCOMM® is a registered trademark of QUALCOMM Incorporated. Used under license.

Other trademarks are the property of their respective owners.

Contact Information

Support Desk:	Phone:	1-877-231-1144
	Hours:	5:00 AM to 5:00 PM Pacific Time, Monday to Friday, except US Holidays
	E-mail:	support@sierrawireless.com
Sales Desk:	Phone:	1-510-624-4200 1-604-232-1488
	Hours:	8:00 AM to 5:00 PM Pacific Time
	E-mail:	MobileandM2Msales@sierrawireless.com
Post:	Sierra Wireless America 39677 Eureka Drive Newark, CA 94560 USA Sierra Wireless 13811 Wireless Way Richmond, BC Canada V6V 3A4	
Fax:	1-510-624-4299 1-604-231-1109	
Web:	www.sierrawireless.com	

Consult our website for up-to-date product descriptions, documentation, application notes, firmware upgrades, troubleshooting tips, and press releases:

www.sierrawireless.com

Revision number	Release date	Changes
1.0	April 2011	FDQN Support for IPsec Application Note created.
1.1	June 2011	FDQN Support for IPsec Application Note revised and released. Limitations, Interoperability, and Appendix sections added.

FQDN Support for IPsec

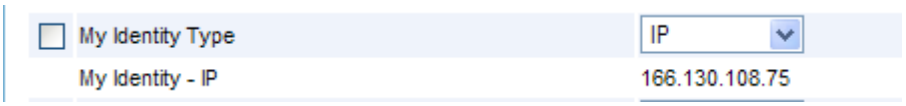
FQDN (fully qualified domain name) is a method of identification used with the Internet Key Exchange (IKE) When the identification date is received from a peer host, IKE will search a database of pre-shared keys for the specific key that is associated with the identification data.

Two methods of identification are included in FQDN. These methods only work in the Aggressive Mode:

- Domain Names: A fully qualified domain name is used for identification. For example, my_modem.eairlink.com
- User Domain Names: A user domain name in the form of an e-mail address. This is useful if multiple users have different pre-shared keys on a single host. For example, AleosRules@sierrawireless.com.

FQDN User Interface

The fields applicable to FQDN (see following figures) appear on the ACEmanager/VPN tabs. Sierra Wireless legacy products support FQDN on two VPN tunnels simultaneously.



Or ...

Applicability

- PinPoint, Raven, and MP platforms: ALEOS 4.0.9 and later versions
- GX400 platforms: ALEOS 4.2.1 and later versions.

Interoperability

- Cisco 2901
- SonicWALL 240

Appendix A: Cisco Router Configuration

Cisco 2901 Configuration Script

Cisco 2901 configuration

_____

```
Fr
testlab-2901#sh runn
Building configuration...

Current configuration : 6427 bytes
!
! Last configuration change at 15:09:29 UTC Sat May 28 2011 !
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname testlab-2901
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
no aaa new-model
!
!
!
!
no ipv6 cef
ip source-route
ip cef
!
!
!
!
ip domain name eairlink.com
ip name-server 64.163.70.23
!
multilink bundle-name authenticated
!
!
!
crypto pki trustpoint TP-self-signed-3538810357  enrollment selfsigned  subject-name
      cn=IOS-Self-Signed-Certificate-3538810357
 revocation-check none
 rsakeypair TP-self-signed-3538810357
```

```
!
!
crypto pki certificate chain TP-self-signed-3538810357  certificate self-signed 01
  3082024B 308201B4 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33353338 38313033 3537301E 170D3131 30343034 32333134
  35375A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 35333838
  31303335 3730819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100DF59 59B6AF44 512FF1E1 AE79088A 3A8785B0 EB4F453F 11117BD6 E733CB5C
  2DA5378A 88039DB0 F6063B11 1617D69A A90EAD04 633273CD 55171EE8 BE7037D0
  0784B524 A0347FE4 AEA7AE23 66CA522D A2B0EB93 C1CFF270 D15F9EF0 7CF87D9F
  8BD57AEB CBC50F96 3CA05EFB A4CF18CD 17614D00 BCD2E736 A226C1D9 67AE07A9
  9D630203 010001A3 73307130 0F060355 1D130101 FF040530 030101FF 301E0603
  551D1104 17301582 13526F75 7465722E 65616972 6C696E6B 2E636F6D 301F0603
  551D2304 18301680 14492A9F 23258079 DCDBA4DB A544247F 7A71D2D9 9A301D06
  03551D0E 04160414 492A9F23 258079DC DBA4DBA5 44247F7A 71D2D99A 300D0609
  2A864886 F70D0101 04050003 81810000 9770326F 09BCFCD6 6A57E83A 07843075
  C5532CAF E701516D ABBB29A6 4907F86E 55827B20 7733081B 60D7D6BA 931CDE47
  1F4CF367 6EF904BA B4F94D39 3EFC5C71 A073C6B1 654A1D59 39B20200 0DC97B4F
  1B00E079 38BA690B 7B665808 E9AF9B09 3103B26D 6A395059 B481918B 28989163
  38C08E62 5206D1ED 14AA287D E281C9
       quit
license udi pid CISCO2901/K9 sn FTX145004FW !
!
username user privilege 15 secret 5 $1$..Me$3yuwj25zRQHIlMKLV4gm01 username sqa
      privilege 15 secret 5 $1$K9oD$39nSMwFhH9iURE8.UWhbL1 username test privilege
      15 secret 5 $1$TefW$Nh.8mqJkORw8.JBSXXiFy0 username cisco privilege 15 secret 5
      $1$Pzwm$QzkXJH5wS2ykYX3HlhAGa.
!
redundancy
!
!
!
!
crypto isakmp policy 2
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp policy 5
 encr aes 256
 authentication pre-share
 group 2
 lifetime 7200
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
```

```
!
crypto isakmp policy 100
 encr 3des
 authentication pre-share
 group 2
 lifetime 7200
crypto isakmp key 6 cisco12345 hostname cdma421.eairlink.com crypto isakmp identity
      hostname crypto isakmp nat keepalive 20 !
crypto ipsec security-association lifetime seconds 7200 !
crypto ipsec transform-set IOs-IPSEC esp-3des esp-sha-hmac crypto ipsec transform-set
      3DES-MD5 esp-3des esp-sha-hmac crypto ipsec transform-set 3DES-SHA esp-3des
      esp-sha-hmac crypto ipsec transform-set aes128 esp-aes esp-sha-hmac crypto ipsec
      transform-set aes192 esp-aes 192 esp-sha-hmac crypto ipsec transform-set aes256
      esp-aes 256 esp-sha-hmac !
crypto dynamic-map MODEM-DYN-MAP 300
 set transform-set aes128 aes192 aes256 3DES-SHA  match address 100 !
!
>>>>>>>>>>>>>>>>>>>>fqdn configuration>>>>>>>>>>>>>>>>>>>>>>>
crypto map SDM_CMAP_1 1 ipsec-isakmp
 set peer cdma421.eairlink.com dynamic
 set transform-set aes128 aes192 aes256 3DES-SHA  match address 100
>>>>>>>>>>>>>>>>>>>>fqdn configuration>>>>>>>>>>>>>>>>>>>>>>>
!
!
!
!
!
interface GigabitEthernet0/0
 description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-GE 0/0$$ES_WAN$  ip address
      64.163.70.151 255.255.255.0  duplex auto  speed auto  crypto map SDM_CMAP_1  !
!
interface GigabitEthernet0/1
 description 172.16.1.0_LAN_MANAGEMENT$ES_LAN$  ip address 172.16.1.207
      255.255.255.0  ip virtual-reassembly  no ip route-cache cef  no ip route-cache  duplex
      auto  speed auto  !
!
ip forward-protocol nd
!
ip http server
ip http access-class 23
ip http authentication local
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000 !
ip route 0.0.0.0 0.0.0.0 64.163.70.1
!
ip access-list extended cdma421.eairlink.com !
access-list 100 permit ip 172.16.1.0 0.0.0.255 192.168.13.0 0.0.0.255 !
!
!
!
!
!
control-plane
 !
!
```

```
banner exec ^C
% Password expiration warning.
---------------------------------------------------------------------

Cisco Configuration Professional (Cisco CP) is installed on this device and it provides the
      default username "cisco" for  one-time use. If you have already used the username
      "cisco" to login to the router and your IOS image supports the "one-time" user option,
      then this username has already expired.
You will not be able to login to the router with this username after you exit this session.

It is strongly suggested that you create a new username with a privilege level of 15 using
      the following command.

username <myuser> privilege 15 secret 0 <mypassword>

Replace <myuser> and <mypassword> with the username and password you want to use.

---------------------------------------------------------------------
^C
banner login ^C
---------------------------------------------------------------------
Cisco Configuration Professional (Cisco CP) is installed on this device.
This feature requires the one-time use of the username "cisco" with the password "cisco".
      These default credentials have a privilege level of 15.

YOU MUST USE CISCO CP or the CISCO IOS CLI TO CHANGE THESE  PUBLICLY-KNOWN
      CREDENTIALS

Here are the Cisco IOS commands.

username <myuser>  privilege 15 secret 0 <mypassword> no username cisco

Replace <myuser> and <mypassword> with the username and password you want to use.

IF YOU DO NOT CHANGE THE PUBLICLY-KNOWN CREDENTIALS, YOU WILL NOT BE ABLE TO
      LOG INTO THE DEVICE AGAIN AFTER YOU HAVE LOGGED OFF.

For more information about Cisco CP please follow the instructions in the QUICK START
      GUIDE for your router or go to http://www.cisco.com/go/ciscocp
---------------------------------------------------------------------
^C
!
line con 0
 login local
line aux 0
line vty 0 4
 access-class 23 in
 exec-timeout 90 0
 privilege level 15
 password 7 00171A0316490A
 no login
 transport preferred none
 transport input telnet ssh
```

```
line vty 5 15
 access-class 23 in
 privilege level 15
 login local
 transport input telnet ssh
!
scheduler allocate 20000 1000
end

testlab-2901#
```

Appendix B: SonicWALL Router Configuration

SonicWALL 240 Configuration Screenshots

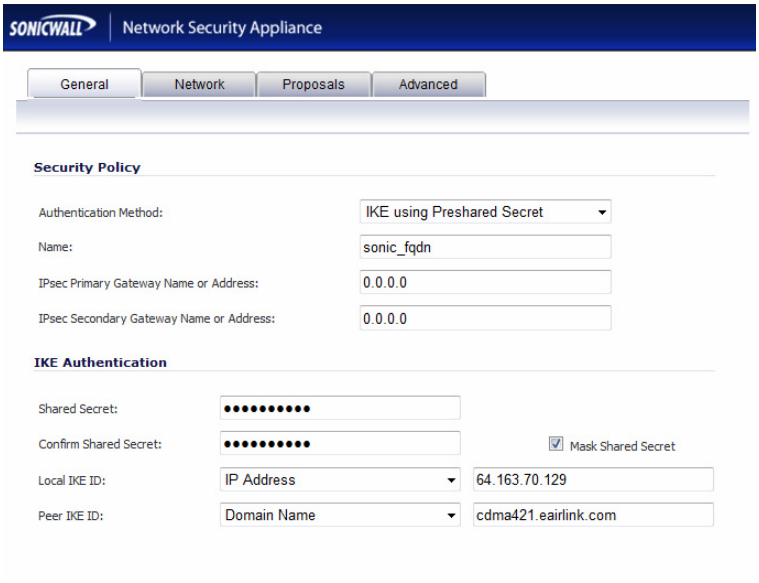


Figure 1: SonicWALL NSA > General tab fields

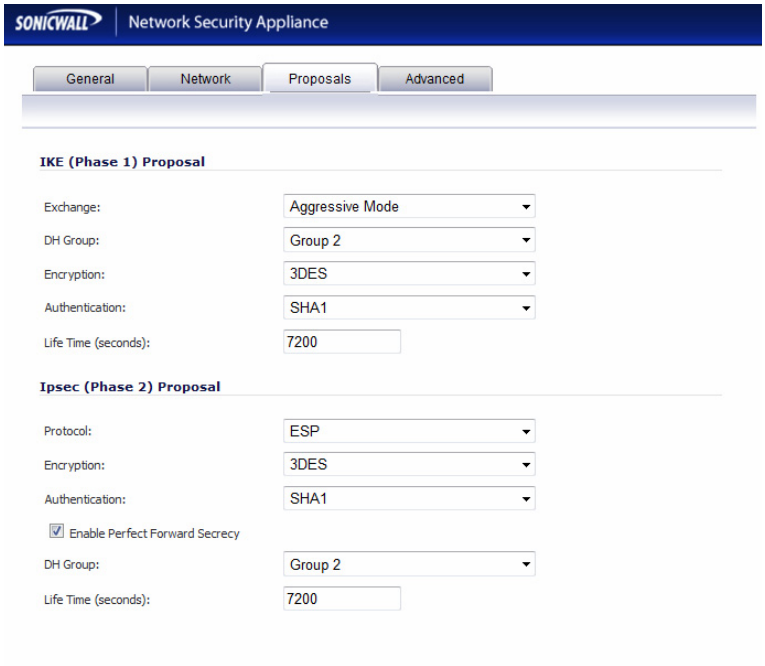


Figure 2: SonicWALL NSA > Proposals tab fields


SIERRA
WIRELESS