



ETM® System v7.1.1

Knowledge Base Article #ETM676

Configuring IPsec Between a UTA Appliance Instance and the Cisco Router

Synopsis

The instructions below detail IPSEC setup between the Cisco router and the UTA Appliance. In the example below, the following IP addresses are used for illustration: router (10.1.50.233) and appliance (10.1.50.229). Substitute your IP addresses.

Configuring IPsec

1. On the UTA Appliance:

- a. Generate keys. One option is to use `/dev/random` with the following commands (sample key output is shown):

```
$ # 192 Bit long key
$ dd if=/dev/random count=24 bs=1 | xxd -ps
24+0 Records ein
24+0 Records aus
9d6c4a8275ab12fbfdcaf01f0ba9dcfb5f424c878e97f888
```

- b. Open the file `/root/setkey.conf` in a text editor such as `vi` and add the following commands to the file:

```
#!/usr/sbin/setkey -f
#Configuration between 10.1.50.229 and 10.1.50.233

#Flush the SAD and SPD
flush;
spdf flush;

#ESP SAs using 192 bit long keys (168 + 24 parity)
add 10.1.50.229 10.1.50.233 esp 301 -m transport -E
0x01234567890123456789012345678901234567890123456789012345678901234567;
add 10.1.50.233 10.1.50.229 esp 401 -m transport -E 3des-cbc
0x0123456789012345678901234567890123456789012345678901234567;

#Security policies
spdadd 10.1.50.229 10.1.50.233 any -P out ipsec
esp/transport//require;

spdadd 10.1.50.233 10.1.50.229 any -P in ipsec
esp/transport//require;
```

IMPORTANT: These keys are for illustration only. Generate your own secure keys.



- c. Execute the following commands to execute the file:

```
# setkey -FP
# setkey -f /root/setkey.conf
```

- d. This configuration is lost upon Appliance restart unless you set the file to execute automatically upon restart. To do so, modify the file **/etc/rc3.d/S99local** and add the following lines:

```
setkey -FP
setkey -f /root/setkey.conf
```

2. In the router's configuration, add the commands below in the order shown, using the same keys and IP addresses you used in the Appliance configuration:

```
access-list 101 permit ip host 10.1.50.233 host 10.1.50.229
```

```
crypto ipsec transform-set uta-50-229 esp-3des
mode transport require
no crypto ipsec transform-set default
```

```
crypto map mymap 10 ipsec-manual
set peer 10.1.50.229
set session-key inbound esp 301 cipher
0123456789012345678901234567890123456789012345678901234567
set session-key outbound esp 401 cipher
0123456789012345678901234567890123456789012345678901234567
set transform-set uta-50-229
match address 101
```

```
interface GigabitEthernet0/0/0
ip address 10.1.50.233 255.255.255.0
negotiation auto
crypto map mymap
```

SecureLogix Corporation

13750 San Pedro, Suite 820 • San Antonio, Texas 78232 • (210) 402-9669 • www.securelogix.com

Support (877) SLC-4HELP • EMAIL support@securelogix.com • <http://support.securelogix.com>

ETM, We See Your Voice, SecureLogix, SecureLogix Corporation, and the SecureLogix Emblem are registered trademarks or registered trademarks and registered service marks of SecureLogix Corporation in the U.S.A. and other countries. PolicyGURU is a trademark of SecureLogix Corporation in the U.S.A. and other countries. All other trademarks mentioned herein are believed to be trademarks of their respective owners.

© Copyright 2014 SecureLogix Corporation. All Rights Reserved. SecureLogix technologies are protected by one or more of the following patents: US 6,226,372 B1, US 6,249,575 B1, US 6,320,948 B1, US 6,687,353 B1, US 6,718,024 B1, US 6,760,420 B2, US 6,760,421 B2, US 7,133,511 B2, US 7,231,027 B2, US 7,440,558 B2, US 8,150,013 B2, CA 2,354,149, DE 1,415,459 B1, FR 1,415,459 B1, and GB 1,415,459 B1.

