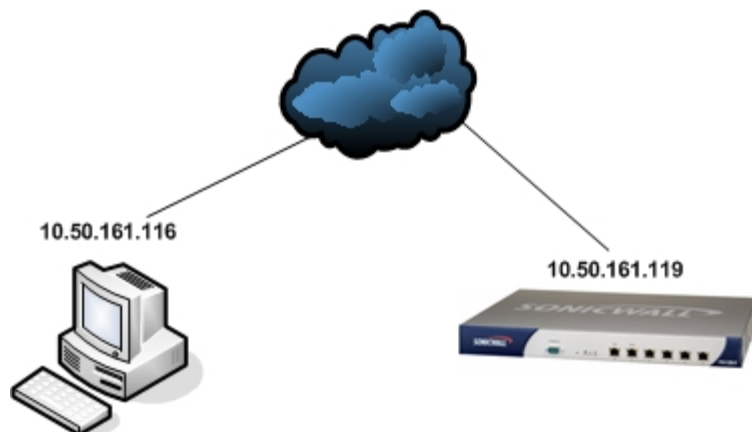


Tech Note

VPN

SonicOS Enhanced to Openswan Using Aggressive Mode IKE with PreShared Key

Deployment Scenario:



Linux machine with Openswan

SonicWALL firewall with SonicOS Enhanced 3.X

[Openswan ipsec.conf](#)

Configure the connection in the ipsec.conf file:

```
conn stephanie
    type=tunnel
    auto=add
    auth=esp
    pfs=no
    authby=secret
    keyingtries=0
    left=10.50.161.116
    leftid=@linux
    leftsubnet=10.50.161.116/32
    right=68.231.47.142
    rightsubnet=192.168.168.0/24
    rightid=@0006B11C3B24
    esp=3des-sha1
    keyexchange=ike
    ike=3des-sha1
    aggrmode=yes
```

connection name

Linux machine's IP address

Linux machine's local IKE ID (SonicWALL's Peer IKE ID)

Linux machine's IP and Subnet Mask

SonicWALL's WAN IP address

Destination network (usually SonicWALL's LAN subnet)

Peer IKE ID (SonicWALL's Local IKE ID)

configures connection for aggressive mode

[Openswan ipsec.secrets](#)

Create an entry in the ipsec.secrets file:

```
@linux @000BB11C3B24 : PSK "sonic"
```

format: (leftid) (rightid) : PSK "preshared key"



Tech Note

SonicOS Enhanced 3.X

Configure the Security Association on the SonicWALL:

Address Object

Name:	<input type="text" value="Steph"/>
Zone Assignment:	<input type="text" value="VPN"/>
Type:	<input type="text" value="Host"/>
IP Address:	<input type="text" value="10.50.161.116"/>

Security Association

General	Network	Proposals	Advanced
Security Policy			
IPSec Keying Mode:	<input type="text" value="IKE using Preshared Secret"/>		
Name:	<input type="text" value="Openswan"/>		
IPSec Primary Gateway Name or Address:	<input type="text" value="0.0.0.0"/>		
IPSec Secondary Gateway Name or Address:	<input type="text" value="0.0.0.0"/>		
Shared Secret:	<input type="text" value="sonic"/>		
Local IKE ID (optional):	<input type="text" value="Domain Name"/>	<input type="text" value="0006B11C3B24"/>	
Peer IKE ID (optional):	<input type="text" value="Domain Name"/>	<input type="text" value="linux"/>	

General	Network	Proposals	Advanced
Local Networks			
<input checked="" type="radio"/>	Choose local network from list	<input type="text" value="LAN Primary Subnet"/>	
<input type="radio"/>	Local network obtains IP addresses using DHCP through this VPN Tunnel		
<input type="radio"/>	Any address		
Destination Networks			
<input type="radio"/>	Use this VPN Tunnel as default route for all Internet traffic		
<input type="radio"/>	Destination network obtains IP addresses using DHCP through this VPN Tunnel		
<input checked="" type="radio"/>	Choose destination network from list	<input type="text" value="Steph"/>	

General	Network	Proposals	Advanced
IKE (Phase 1) Proposal			
Exchange:	<input type="text" value="Aggressive Mode"/>		
DH Group:	<input type="text" value="Group 5"/>		
Encryption:	<input type="text" value="3DES"/>		
Authentication:	<input type="text" value="SHA-1"/>		
Life Time (seconds):	<input type="text" value="28800"/>		
Ipsec (Phase 2) Proposal			
Protocol:	<input type="text" value="ESP"/>		
Encryption:	<input type="text" value="3DES"/>		
Authentication:	<input type="text" value="SHA-1"/>		
<input type="checkbox"/>	Enable Perfect Forward Secrecy		
DH Group:	<input type="text" value="Group 5"/>		
Life Time (seconds):	<input type="text" value="28800"/>		

General	Network	Proposals	Advanced	
Advanced Settings				
<input type="checkbox"/>	Enable Keep Alive			
<input type="checkbox"/>	Suppress automatic Access Rules creation for VPN Policy			
<input type="checkbox"/>	Require authentication of VPN clients by XAUTH			
	User group for XAUTH users:	<input type="text" value="--Select a user group--"/>		
<input type="checkbox"/>	Enable Windows Networking (NetBIOS) Broadcast			
<input type="checkbox"/>	Enable Multicast			
<input type="checkbox"/>	Apply NAT Policies			
	Translated Local Network:	<input type="text" value="--Select Translated Local Network--"/>		
	Translated Remote Network:	<input type="text" value="--Select Translated Remote Network--"/>		
Management via this SA:	<input type="checkbox"/>	HTTP	<input type="checkbox"/>	HTTPS
User login via this SA:	<input type="checkbox"/>	HTTP	<input type="checkbox"/>	HTTPS
Default LAN Gateway (optional):	<input type="text" value="0.0.0.0"/>			
VPN Policy bound to:	<input type="text" value="Interface WAN"/>			



Tech Note

Testing / Troubleshooting

Add the connection, bring the tunnel up, and check the status of the tunnel in Openswan:

Make sure Pluto (the IKE daemon) is started:

```
[root@linux / ]# lsof -i -n if pluto is started, this command will show the processes  
[root@linux / ]# service ipsec start this will start the service
```

Add the connection:

```
[root@linux / ]# ipsec auto --add stephanie 'ipsec auto --add (connection name from ipsec.conf)'
```

Bring the tunnel up:

```
[root@linux / ]# ipsec auto --up stephanie 'ipsec auto --up (connection name from ipsec.conf)'
```

A successful connection will show similar messages in /var/log/secure:

```
104 "stephanie" #3: STATE_MAIN_I1: initiate  
106 "stephanie" #3: STATE_MAIN_I2: sent MI2, expecting MR2  
003 "stephanie" #3: ignoring informational payload, type IPSEC_INITIAL_CONTACT  
004 "stephanie" #3: STATE_MAIN_I4: ISAKMP SA established {auth=OAKLEY_PRESHARED_KEY  
cipher=oakley_3des_cbc_192 prf=oakley_md5 group=modp1024}  
117 "stephanie" #4: STATE_QUICK_I1: initiate  
004 "stephanie" #4: STATE_QUICK_I2: sent QI2, IPsec SA established {ESP=>0x7bbd6d25 <0x36288d40 xfrm=3DES_0-  
HMAC_MD5 NATD=none DPD=none}
```

Errors:

```
[root@linux etc]# ipsec auto --add group  
ipsec_auto: fatal error in "": (/etc/ipsec.conf, line 121) did not find conn section(s) "stephanie"  
The 'stephanie' connection wasn't found in ipsec.conf. Make sure the connection is configured in ipsec.conf. The connection name in the command 'ipsec auto --add stephanie' is case sensitive.
```

```
linux pluto[3584]: "stephanie" #13: Can't authenticate: no preshared key found for '10.50.161.116' and `10.50.161.119'.  
There's no preshared key defined in ipsec.secrets for this connection. Check the settings in ipsec.secrets.
```

```
linux pluto[3584]: "stephanie" #13: no acceptable Oakley Transform  
Check the transforms \(esp=3des sha1, ike=3des sha1\) in the ipsec.conf file.
```

