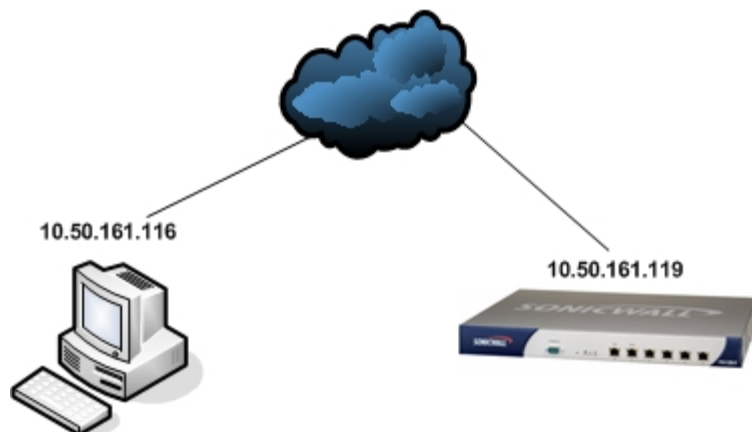


Tech Note

VPN

SonicOS Enhanced to Openswan Using GroupVPN with XAUTH

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 group
  type=tunnel
  left=10.50.161.116
  leftsubnet=10.50.161.116/32
  leftid=@GroupVPN
  leftxauthclient=yes
  right=10.50.161.119
  rightsubnet=192.168.168.0/24
  rightid=@0006B11C3B24
  rightxauthserver=yes
  keyingtries=0
  pfs=no
  auto=add
  auth=esp
  esp=3des-sha1
  ike=3des-sha1
  xauth=yes
  authby=secret
  aggrmode=yes
```

connection name

IP address of Linux machine

IP address and 32-bit subnet mask of Linux machine

Local ID - this is case sensitive

WAN IP address of SonicWALL

Destination network (usually LAN subnet of SonicWALL)

Peer ID - SonicWALL's Unique Firewall Identifier

[Openswan ipsec.secrets](#)

Create an entry in the ipsec.secrets file:

```
@GroupVPN @0006B11C3B24 : PSK "grouppassword"
```

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



Tech Note

SonicOS Enhanced 3.X

Configure the WAN GroupVPN Security Association and create a user with access to the GroupVPN with XAUTH on the SonicWALL:

General Proposals Advanced Client

Security Policy

IPSec Keying Mode: IKE using Preshared Secret

Name: GroupVPN

Shared Secret: grouppassword

General Proposals Advanced Client

IKE (Phase 1) Proposal

DH Group: Group 5

Encryption: 3DES

Authentication: SHA1

Life Time (seconds): 3600

Ipsec (Phase 2) Proposal

Protocol: ESP

Encryption: 3DES

Authentication: SHA1

Enable Perfect Forward Secrecy

DH Group: Group 5

Life Time (seconds): 28800

General Proposals Advanced Client

Advanced Settings

Enable Windows Networking (NetBIOS) Broadcast

Enable Multicast

Management via this SA: HTTP HTTPS

Default Gateway: 0.0.0.0

Client Authentication

Require Authentication of VPN Clients via XAUTH

User Group for XAUTH users: Trusted Users

Allow Unauthenticated VPN Client Access: --Select Local Network--

General Proposals Advanced Client

User Name and Password Caching

Cache XAUTH User Name and Password on Client: Never

Client Connections

Virtual Adapter settings: None

Allow Connections to: Split Tunnels

Set Default Route as this Gateway

Require Global Security Client for this Connection

Client Initial Provisioning

Use Default Key for Simple Client Provisioning

Settings Groups VPN Access

User Settings

Name: shelbig

Password: [masked]

Confirm Password: [masked]

Comment:

Settings Groups VPN Access

Group Memberships

User Groups:	Member Of:
Content Filtering Bypass	Everyone
Guest Services	Trusted Users
Limited Administrators	

Add All -> <- Remove All

Settings Groups VPN Access

VPN Client Access Networks

Networks:	Access List:
All Interface IP	LAN Primary Subnet
All LAN Management IP	
All WAN IP	
All WAN Management IP	
Default SonicPoint ACL Allow Gro	

-> <- Remove All



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 / ]# lsuf -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 group 'ipsec auto --add (connection name from ipsec.conf)'
```

Bring the tunnel up:

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

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

```
112 "group" #9: STATE_AGGR_I1: initiate  
004 "group" #9: STATE_AGGR_I2: sent AI2, ISAKMP SA established {auth=OAKLEY_PRESHARED_KEY  
cipher=oakley_3des_cbc_192 prf=oakley_sha group=modp1536}  
041 "group" #9: group prompt for Username:  
Name enter: here you will be prompted for XAUTH username  
040 "group" #9: group prompt for Password:  
Enter secret: here you will be prompted for XAUTH password  
004 "group" #9: STATE_XAUTH_I1: XAUTH client - awaiting CFG_set  
117 "group" #10: STATE_QUICK_I1: initiate  
004 "group" #10: STATE_QUICK_I2: sent QI2, IPsec SA established {ESP=>0xb61e699e <0x9cb1fe74 xfrm=3DES_0-  
HMAC_SHA1 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) "group"  
The 'group' 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 group' is case sensitive.
```

```
linux pluto[3584]: "group" #13: Can't authenticate: no preshared key found for '@GroupVPN' and '@0006B1142228'.  
There's no preshared key defined in ipsec.secrets for this connection. Check the settings in ipsec.secrets.
```

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

