

IPSec between uSysCom 3GAT and Cisco PIX Firewall

Scope

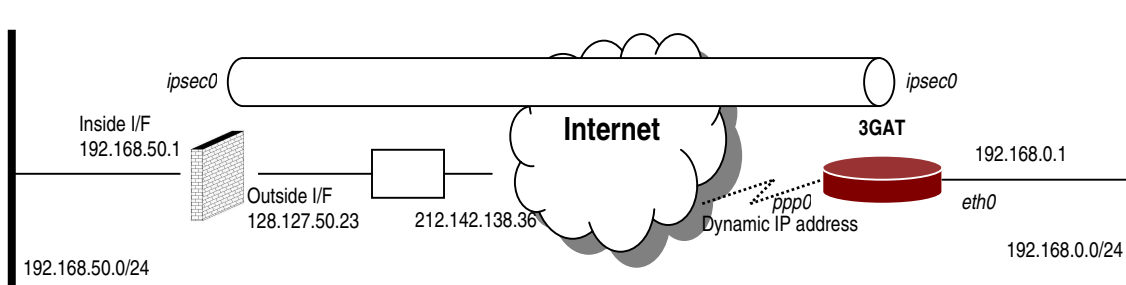
This application note describes the main steps in order to set up an IPSec tunnel between uSysCom 3GAT wireless routers and a Cisco PIX router. In this sample configuration, the 3GATE receives from the network carrier a dynamic public IP address and connects to a central PIX that is configured to accept dynamic IPSec connections. To do so, PIX firewall needs to be configured to dynamically accept connections from anywhere knowing the pre-shared key.

This document assumes that the reader is familiar with both, IPSec/IKE concepts and the Cisco PIX command line interface.

Network architecture

Next figure shows the architecture that is to be described. On one end, a private LAN is behind the Cisco PIX firewall inside interface. A LAN behind the 3GAT wireless router is on the other end. It is important to note that the Cisco PIX firewall has a public address. More accurately, the Cisco PIX firewall is behind a NAT device which translates the public IP address, 212.142.138.36 into the Cisco PIX outside interface IP address 128.127.50.23.

Finally, it should be noted that the 3GAT gets a public dynamic IP address.



The tunnel is defined by the following parameters:

IKE Parameter	Value
Identification	IP Address
Authentication method (Pre-shared key)	"usyscom"
Exchange mode for phase 1	Main mode
Encryption Algorithm	3DES
Authentication algorithm	MD5
Diffie Hellman	DH2
IKE LifeTime (seconds)	86.400 s

IPSec Parameter	Value
Security Protocol	ESP
Encryption Algorithm	3DES
Authentication algorithm	MD5
IPSec LifeTime (seconds)	28.800 s
PFS Group	None

Cisco PIX Configuration

The whole PIX configuration is depicted below. We have highlighted the main configuration commands involved in order to accept remote IPSec connections from 3GAT routers.

```
PIX Version 6.3(4)
interface ethernet0 auto
interface ethernet1 100full
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 7fTJ9W4fig2zvTUI encrypted
hostname pixfirewall
domain-name ussyscom.com
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names

! Remote LAN behind 3 GAT router
name 192.168.0.0 remoteBranch

! ACL to avoid NAT (Network Address Translation) on IPSec Packets
access-list inside_nat0_outbound permit ip 192.168.50.0 255.255.255.0 remoteBranch
255.255.255.0

!ACL to determine the traffic pattern for IPSec
access-list outside_cryptomap_dyn_20 permit ip 192.168.50.0 255.255.255.0 remoteBranch
255.255.255.0

pager lines 24
icmp permit any outside
icmp permit any inside
mtu outside 1500
mtu inside 1500

ip address outside 128.127.50.23 255.255.0.0

ip address inside 192.168.50.1 255.255.255.0

ip audit info action alarm
ip audit attack action alarm
pdm location remoteBranch 255.255.255.0 outside
pdm location remoteBranch 255.255.255.0 inside
pdm logging informational 100
pdm history enable
arp timeout 14400
global (outside) 1 interface

! Do not NAT on IPSec packets
nat (inside) 0 access-list inside_nat0_outbound

nat (inside) 1 0.0.0.0 0.0.0.0 0 0

route outside 0.0.0.0 0.0.0.0 128.127.50.138 1

timeout xlate 0:05:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
```

```
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
http server enable
http 128.127.0.0 255.255.0.0 outside
http 192.168.50.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable

! This command avoids conduit on the IPsec encrypted traffic
sysopt connection permit-ipsec

! IPsec Encryption type
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto dynamic-map outside_dyn_map 20 match address outside_cryptomap_dyn_20
crypto dynamic-map outside_dyn_map 20 set transform-set ESP-3DES-MD5
crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map

! Binding IPsec engine on the outside interface
crypto map outside_map interface outside

! Enabling ISAKMP key-exchange
isakmp enable outside

! ISAKMP policy for connecting to Central PIX
isakmp key ***** address 0.0.0.0 netmask 0.0.0.0 no-xauth no-config-mode
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400

telnet 128.127.0.0 255.255.0.0 outside
telnet 192.168.50.0 255.255.255.0 inside
telnet remoteBranch 255.255.255.0 inside
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd address 192.168.50.100-192.168.50.125 inside
dhcpd dns 128.127.50.8
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd domain usyscom.com
dhcpd auto_config outside
dhcpd enable inside
username root nopassword privilege 15
terminal width 80
Cryptochecksum:79b0f2ee2bd7ce57effc41ba8dd85cfb
: end
[OK]
```

3GAT Configuration

This paragraph focuses on the IPSec configuration parameters. For additional info, please refer to the 3GAT SW Configuration Guide.

- In the main menu, choose TUNNELING option.
- Tunnel parameters need to be defined in *TUNNEL DEFINITION* section. Remember tunnel identifier, `to_firewallpix`, as it must be the same used when defining tunnel security policies.

#	Tunnel Id	Type	Local Network	Remote Gw	Remote Network	
1	to_firewallpix	ipsec	192.168.0.0/255.255.255.0	212.142.138.36	192.168.50.0/255.255.255.0	Delete
2	Add					

- In the PRESHARED KEYS, “usyscom” preshared key is defined for the peer IP 212.142.138.36.

#	Peer IP	Password	
1	212.142.138.36	usyscom	Delete
2	Add		

- The IKE policy should reflect previously agreed parameters:

#	Peer ID Type	Peer ID Value	Passive Exchange	Mode	Cipher Alg.	Hash Alg.	Auth. Method	DH-Group	Lifetime	Description	
1	address	212.142.138.36	<input type="checkbox"/>	main	3des	md5	pre_shared_key	modp1024	86400	ike_0	Delete
2	Add										

- Finally, IPSec Association should be configured for ESP protocol, being the authentication and ciphering algorithms MD5 and 3DES respectively. Remember to use the same tunnel identifier, `to_firewallpix`, as when defining the tunnel.

#	Tunnel Id	Protocol	Cipher Alg.	Hash Alg.	PFS	Lifetime	
1	to_firewallpix	esp	3des	hmac_md5	none	28800	Delete
2	Add						

IPSec Tunnel / Established

To initiate the tunnel, send a ping from a machine behind 3GAT to a machine behind the PIX firewall. Once the IP Security is successfully negotiated, the tunnel will be established between both subnetworks.