Technical Guide

# How to Configure an AR-Series Firewall as a Secure VPN Gateway and an AMF Node

## Introduction

The Allied Telesis AR-Series Firewalls are versatile network appliances. They can operate as Next Generation Firewalls, VPN gateways, multi-protocol routers, and remote access concentrators. They can also participate fully in the Allied Telesis Management Framework (AMF).

This How to note is a step-by-step configuration guide for setting up a pair of AR-Series Firewalls for a common inter-office connection scenario.

The scenario involves a remote office connecting via site-to-site IPsec VPN to a main office. The VPN configuration includes both a primary link over wired Ethernet and, at the remote office, a backup link over a cellular network.

In addition, the main office firewall is configured to allow secure client-to-site SSL/TLS connections from roaming workers using OpenVPN.

Both firewalls are also configured to participate in AMF networks.

The configurations provided here are designed to be a starting point for network engineers to use when configuring similar scenarios using Allied Telesis AR-Series Firewalls.

AlliedWare Plus™
OPERATING SYSTEM

# Contents

## Related documents

You also may find the following AlliedWare Plus™ documents useful:

- AMF feature overview and configuration guide
- OpenVPN feature overview and configuration guide
- NGFW GUI overview and configuration guide
- IPSec feature overview and configuration guide

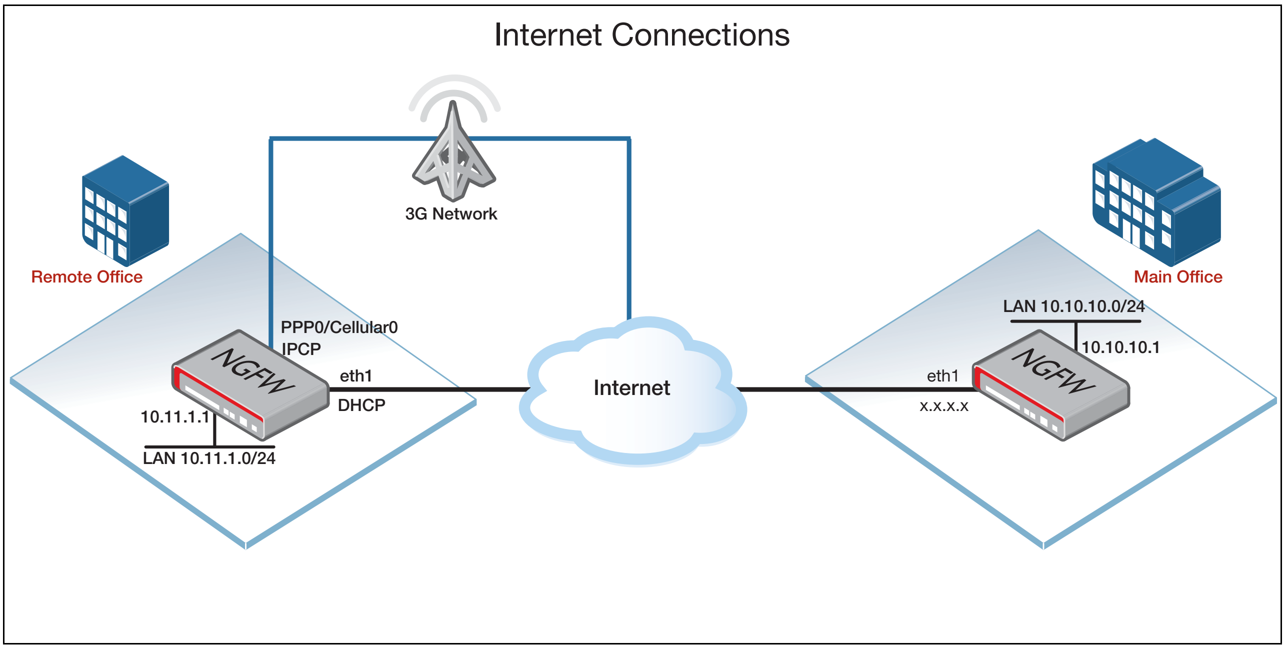
## Which products and software version does it apply to?

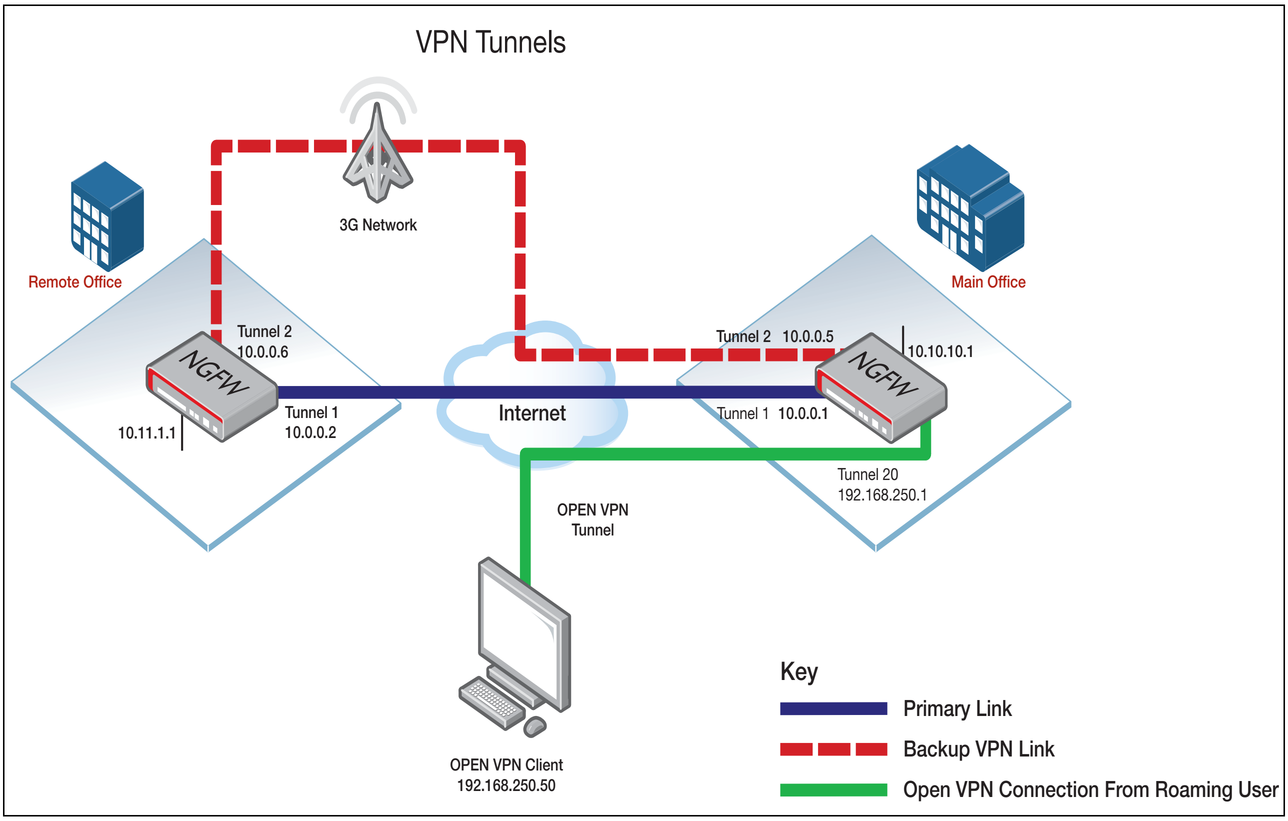
This guide applies to the AlliedWare Plus AR2010V and AR2050V VPN Firewalls, and AR3050S and AR4050S NGFWs, running **v5.4.6-1** or later.

# Network Diagram

The network is represented in two diagrams.

- The first diagram shows the physical connections to each of the firewalls.
- The second diagram shows all the VPN tunnels that are configured in the network.





# Basic Firewall Configuration

This section describes the configuration required to set up the two AR-Series Firewalls as secure Internet gateways for their respective offices.

## Main office firewall

The basic configuration to set up the AR-Series Firewall as a secure Internet gateway is straightforward.

The key items that need to be configured are:

- Hostname
- IP addresses for vlan1 (internal) and eth1 (WAN - external)
- Firewall
- NAT
- IP route table
- Passwords

Then, at the end, the configuration is saved to a file, that is set to be the startup configuration file.

Firstly, configure a **hostname**. This step is important, as it is used later on to allow the router to participate in the AMF network.

### Hostname configuration

```
awplus> ena
awplus#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
awplus(config)#hostname Main_Office
```

### IP address configuration

IP addresses are applied to the WAN interface (eth1) and the LAN interface (vlan1). The IP address x.x.x.x represents the static WAN IP address allocated by the Internet service provider.

```
Main_Office(config)#interface eth1
Main_Office(config-if)#description wan
Main_Office(config-if)#ip address x.x.x.x/x
Main_Office(config-if)#int vlan1
Main_Office(config-if)#description lan
Main_Office(config-if)#ip address 10.10.10.1/24
Main_Office(config-if)#exit
```

### Firewall configuration

Two firewall zones are created:

- private—containing the local network entity accessed via the vlan1 interface.
- public—containing the Internet and WAN network for connection to the Internet, via the eth1 WAN interface.

Firewalls rules are created:

- allowing all traffic between addresses within the private zone
- allowing traffic from the local network within the private zone to the public zone

The firewall is then enabled via the **protect** command.

```
Main_Office(config)#zone private
Main_Office(config-zone)#network local
Main_Office(config-network)#ip subnet 10.10.10.0/24 interface vlan1
Main_Office(config-network)#exit
Main_Office(config-zone)#exit
Main_Office(config)#zone public
Main_Office(config-zone)#network internet
Main_Office(config-network)#ip subnet 0.0.0.0/0 interface eth1
Main_Office(config-network)#network wan
Main_Office(config-network)#ip subnet x.x.x.x/x
Main_Office(config-network)#host router
Main_Office(config-host)#ip address x.x.x.x
Main_Office(config-host)#exit
Main_Office(config-network)#exit
Main_Office(config-zone)#exit
Main_Office(config)#firewall
Main_Office(config-firewall)#rule 10 permit any from private to private
Main_Office(config-firewall)#rule 20 permit any from private.local to public
Main_Office(config-firewall)#protect
Main_Office(config-firewall)#exit
```

### NAT configuration

Traffic exchanged between the private and public zones has NAT applied. So, the WAN IP address is used as the source address of LAN traffic going out to the Internet.

```
Main_Office(config)#nat
Main_Office(config-nat)#rule 10 masq any from private.local to public
Main_Office(config-nat)#enable
Main_Office(config-nat)#exit
```

### IP route configuration

A single default route is directed out the WAN interface, toward the ISP's gateway router IP x.x.x.x.

```
Main_Office(config)#ip route 0.0.0.0/0 x.x.x.x
```

### Change password

The default password on the manager user account should be replaced by a non-default password.

```
Main_Office(config)#username manager password <new password>
```

### Save the configuration

The configuration is saved to a new file name, and that file is set as the startup config.

```
Main_Office(config)#exit
Main_Office#copy running-config <new_file_name>.cfg
Main_Office#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Main_Office(config)#boot config-file <new_file_name>.cfg
Main_Office(config)#exit
```

Then to save after this step use the commands:

```
Main_Office#copy running-config startup-config
#OR
Main_Office#write
```

## Remote office (with 3G backup)

The AR-Series Firewall at the remote site is also configured as a secure Internet gateway. The extra feature in this case is that there is a backup Internet connection via the 3G/4G cellular network.

The items in the configuration are:

- Hostname
- Cellular configuration
- IP addresses for eth1 (primary WAN) and cellular0 (backup WAN)
- Firewall
- NAT
- IP route configuration
- Passwords

Then, at the end, the configuration is saved to a file, that is set to be the startup configuration file.

### Hostname configuration

```
awplus> ena
awplus#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
awplus(config)#hostname Remote
```

## Cellular configuration

A PPP (Point-to-Point Protocol) link is configured to provide the data encapsulation over the 3G cellular connection.

To enable the cellular link to be successfully connected, the interface needs to be configured with the APN (Access Point Name), that can be obtained from the cellular carrier provider.

```
Remote(config)#interface cellular0
Remote(config-if)#encapsulation ppp 0
Remote(config-if)#apn <cellular carrier APN>
```

## IP address configuration

IPv4 interfaces are configured on the VLAN1, eth1, and PPP0 (over cellular) interfaces.

Note that the eth1 interface is configured to obtain its IP address by DHCP, and the PPP0 interface is configured to receive its IP address by PPP IPCP negotiation. So, both of these interfaces have dynamic IP addresses.

```
Remote(config-if)#interface vlan1
Remote(config-if)#description LAN
Remote(config-if)#ip address 10.11.1.1/24
Remote(config-if)#exit
Remote(config)#interface eth1
Remote(config-if)#description wan_Wired
Remote(config-if)#ip address dhcp
Remote(config-if)#exit
Remote(config)#interface ppp0
Remote(config-if)#description wan_3g
Remote(config-if)#ppp ipcp dns request
Remote(config-if)#keepalive
Remote(config-if)#ip address negotiated
Remote(config-if)#ip tcp adjust-mss pmtu
Remote(config-if)#exit
```

## Firewall configuration

Two zones are created:

- Private—the LAN accessed via the VLAN1 interface.
- Public—the Internet, accessed via the eth1 or PPP0 interface.

Two firewall rules are created:

- Allowing all traffic between addresses in the private zone.
- Allowing traffic from the private zone to the public zone.

```
Remote(config)#zone private
Remote(config-zone)#network local
Remote(config-network)#ip subnet 10.11.1.0/24 interface vlan1
Remote(config-network)#exit
Remote(config-zone)#exit
Remote(config)#zone public
Remote(config-zone)#network wan
Remote(config-network)#ip subnet 0.0.0.0/0 interface eth1
Remote(config-network)#ip subnet 0.0.0.0/0 interface ppp0
Remote(config-network)#host router
Remote(config-host)#ip address dynamic interface eth1
Remote(config-host)#ip address dynamic interface ppp0
Remote(config-host)#exit
Remote(config-network)#exit
Remote(config-zone)#exit
Remote(config)#firewall
Remote(config-firewall)#rule 10 permit any from private to private
Remote(config-firewall)#rule 20 permit any from private.local to public
Remote(config-firewall)#protect
Remote(config-firewall)#exit
```

### NAT configuration

Traffic exchanged between the private and public zones has NAT applied. So, the WAN IP address is used as the source address of LAN traffic going out to the Internet. The source IP that is selected for NAT translations of the data going to the Internet is determined automatically, based on the egress interface through with the data passes. If the WAN interface fails over from eth1 to PPP0, NAT will automatically cut over from using the eth1 IP address to using the PPP0 IP address as the source IP it applies to the outgoing packets.

```
Remote(config)#nat
Remote(config-nat)#rule 10 masq any from private.local to public
Remote(config-nat)#enable
Remote(config-nat)#exit
```

### IP route configuration

A static default route is configured over the PPP0 interface.

A lower-metric default route is created dynamically over the eth1 interface when that interface receives its DHCP lease from the ISP.

```
Remote(config)#ip route 0.0.0.0/0 ppp0
```

### Change password

The default password on the manager user account should be replaced by a non-default password.

```
Remote(config)#username manager password <new password>
```

### Save the configuration

The configuration is saved to a new file name, and that file is set as the startup config.

```
Remote(config)#exit
Remote#copy running-config <new_file_name>.cfg
Remote#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Remote(config)#boot config-file <new_file_name>.cfg
Remote(config)#exit
```

Then to save after this step use the commands:

```
#Remote#copy running-config startup-config
#Or
Remote#write
```

Now test the Internet connectivity for each firewall - bear in mind that with the current configurations the AR-Series Firewall device itself will not ping the Internet due to the firewall rules (no rule has been created to explicitly allow traffic exchange between the device itself and the Internet, so that traffic will be dropped by default), so you need to connect a PC to VLAN1 and check that you are connected.

Note: For the 3G connection you can also check that the 3G is connected by running the **show interface brief** and **show ip interface** commands to see if ppp0 is running and has an IP address allocated. If it does, then there is an Internet connection through the cellular network.

# Main Office VPN and Associated Firewall Configuration

### Main office

The following configurations are provided below:

- VPN tunnel
- Firewall
- IP route table
- Failover configuration and scripts

### ISAKMP key configuration

Configure the ISAKMP keys to be used to negotiate the secure IPSEC VPNs between the offices. In this example, the same pre-shared key is used for both VPNs. Each key is mapped to a specific VPN based on the hostname.

```
Main_Office#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Main_Office(config)#crypto isakmp key <samplekey> hostname
remote_wired
Main_Office(config)#crypto isakmp key <samplekey> hostname remote_3g
Main_Office(config)#exit
```

### Tunnel configuration

Two tunnels are configured on the main office AR-Series Firewall. One tunnel is designed to be connected to the wired (Eth1) interface of the remote office firewall, and the other is designed to be connected to the cellular PPP interface of the remote-office firewall.

At the main office, the fixed Ethernet WAN IP is used as the source IP for each VPN to the remote office.

Both tunnels are configured with the command **tunnel destination dynamic**, as the IP addresses of the target interfaces of the remote office are dynamically allocated.

Each incoming VPN connection from the remote office contains a source IP, as well as a tunnel name. The tunnel name and source IP are unique for each incoming VPN. The tunnel name is extracted from the incoming VPN request and matched against the configured **tunnel remote name**, to allow each incoming VPN to be identified and a security association to be formed.

For each **tunnel name** there is also a corresponding **crypto isakmp key <samplekey> hostname <hostname>** command in which the **<hostname>** is the same as the **tunnel name**. This ensures that there is a correspondence between the IPSEC connection, and the appropriate pre-shared ISAKMP key.

So, the chain of correspondence is:

- A tunnel on the remote router is configured with the command **tunnel local name <tunnel name>**.
- When that tunnel initiates a connection it includes **<tunnel name>** in its connection initiation packets.
- The main office router finds **<tunnel name>** in the incoming tunnel initiation packets.
- The main office router uses the tunnel configured with the command **tunnel remote name <tunnel name>** to answer the incoming connection.
- The main office router uses the ISAKMP key configured in the command **crypto isakmp key <samplekey>hostname <tunnel name>** as the ISAKMP key for this connection.

```
Main_Office#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Main_Office(config)#interface tunnel1
Main_Office(config-if)#tunnel source eth1
Main_Office(config-if)#tunnel destination dynamic
Main_Office(config-if)#tunnel remote name remote_wired
Main_Office(config-if)#tunnel protection ipsec
Main_Office(config-if)#tunnel mode ipsec ipv4
Main_Office(config-if)#ip address 10.0.0.1/30
Main_Office(config-if)#exit
Main_Office(config)#interface tunnel2
Main_Office(config-if)#tunnel source eth1
Main_Office(config-if)#tunnel destination dynamic
Main_Office(config-if)#tunnel remote name Remote_3g
Main_Office(config-if)#tunnel protection ipsec
Main_Office(config-if)#tunnel mode ipsec ipv4
Main_Office(config-if)#ip address 10.0.0.5/30
Main_Office(config-if)#exit
```

The next step is to configure the firewall to ensure VPN connections are not blocked.

## Firewall configuration

A number of additions are now made to the firewall configuration:

1. The LAN subnet on the remote office is added to the existing private zone of the main office. This is because the remote Office LAN is just as trusted as the main office LAN.
2. The networks associated with the tunnels are added to the existing private zone.
3. The protocols for ESP, NAT-T encapsulated IPSec, and ISAKMP are defined in the “application” list, so that specific rules for the encrypted traffic can then be created.
4. Rules are created to allow incoming IPSec, ISAKMP, and NAT-T-encapsulated IPSec traffic from the remote office.

```
Main_Office(config)#zone private
Main_Office(config-zone)#network remote_office
Main_Office(config-network)#ip subnet 10.11.1.0/24
Main_Office(config-network)#exit
Main_Office(config-zone)#network tunnel1
Main_Office(config-network)#ip subnet 10.0.0.0/30
Main_Office(config-network)#exit
Main_Office(config-zone)#network tunnel2
Main_Office(config-network)#ip subnet 10.0.0.4/30
Main_Office(config-network)#exit
Main_Office(config-zone)#exit
Main_Office(config)#application esp
Main_Office(config-application)#protocol 50
Main_Office(config-application)#exit
Main_Office(config)#application ipsec_nat_t
Main_Office(config-application)#protocol udp
Main_Office(config-application)#sport 4500
Main_Office(config-application)#dport 4500
Main_Office(config-application)#exit
Main_Office(config)#application isakmp
Main_Office(config-application)#protocol udp
Main_Office(config-application)#sport 500
Main_Office(config-application)#dport 500
Main_Office(config-application)#exit
Main_Office(config)#firewall
Main_Office(config-firewall)#rule 30 permit esp from public to
public.wan.router
Main_Office(config-firewall)#rule 40 permit isakmp from public to
public.wan.router
Main_Office(config-firewall)#rule 50 permit ipsec_nat_t from public to
public.wan.router
Main_Office(config-firewall)#exit
```

### IP route configuration

The primary route to the remote-office LAN subnet is configured via Tunnel1.

```
Main_Office(config)#ip route 10.11.1.0/24 tunnel1
Main_Office(config)#exit
```

## Failover and scripts

To configure failover we need to configure some ping polls, some triggers, and some scripts. Create a file called tunnel_1_down.scp, which brings up the backup tunnel, and moves the route to the remote office LAN over to that tunnel. The content of the file is:

```
ena
con t
int tunnel2
no shut
ex
ip route 10.11.1.0/24 tunnel2
no ip route 10.11.1.0/24 tunnel1
```

Create a file called tunnel_1_up.scp, which takes down the backup tunnel, and moves the route for the remote office LAN back to the primary tunnel. The content of the file is:

```
ena
con t
int tunnel2
shut
ex
no ip route 10.11.1.0/24 tunnel2
ip route 10.11.1.0/24 tunnel1
```

Ping-poll needs to be configured on the firewall. The ping-poll sends pings to the IP address of the far end of the primary tunnel (tunnel1). If the pings fail, then a ping-poll **down** trigger will go off. When the pings start to succeed again (meaning the primary tunnel has recovered), a ping-poll **up** trigger will go off. The required configuration is:

```
Main_Office#configure terminal
Main_Office(config)#ping-poll 1
Main_Office(config-ping-poll)#ip 10.0.0.2
Main_Office(config-ping-poll)#normal-interval 1
Main_Office(config-ping-poll)#up-count 3
Main_Office(config-ping-poll)#fail-count 3
Main_Office(config-ping-poll)#active
Main_Office(config-ping-poll)#exit
```

Lastly, set up the triggers so that when pings to the far end of the primary tunnel fail, the backup tunnel becomes active, and then when the pings succeed again, the VPN traffic is moved back the primary tunnel.The required configuration is:

```
Main_Office(config)#trigger 1
Main_Office(config-trigger)#type ping-poll 1 down
Main_Office(config-trigger)#script 1 tunnel_1_down.scp
Main_Office(config-trigger)#exit
Main_Office(config)#trigger 2
Main_Office(config-trigger)#type ping-poll 1 up
Main_Office(config-trigger)#script 1 tunnel_1_up.scp
Main_Office(config-trigger)#exit
```

# Remote Office VPN and Associated Firewall Configuration

The following configurations are provided below:

- VPN tunnel
- Firewall
- IP route table
- Failover configuration and scripts

Firstly, the ISAKMP pre-shared key is configured, with x.x.x.x representing the fixed WAN IP address of the main office.

### ISAKMP key configuration

```
Remote#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Remote(config)#crypto isakmp key <samplekey> x.x.x.x
```

### Tunnel configuration

Two tunnels are created on the Remote-office AR Series Firewall. One tunnel goes over the wired (Eth1) interface, and the other tunnel goes over the cellular interface, with x.x.x.x representing the fixed WAN IP address of the main office.

The way that the tunnels identify themselves to the target interfaces is via the names configured with the parameter **local name**.

```
Remote(config)#interface tunnel1
Remote(config-if)#tunnel source eth1
Remote(config-if)#tunnel destination x.x.x.x
Remote(config-if)#tunnel local name remote_wired
Remote(config-if)#tunnel protection ipsec
Remote(config-if)#tunnel mode ipsec ipv4
Remote(config-if)#ip address 10.0.0.2/30
Remote(config-if)#exit
Remote(config)#interface tunnel2
Remote(config-if)#tunnel source ppp0
Remote(config-if)#tunnel destination x.x.x.x
Remote(config-if)#tunnel local name remote_3g
Remote(config-if)#tunnel protection ipsec
Remote(config-if)#tunnel mode ipsec ipv4
Remote(config-if)#ip address 10.0.0.6/30
Remote(config-if)#exit
```

### Firewall configuration

A number of additions are now made to the firewall configuration:

1. The LAN subnet on the main office is added to the existing private zone of the remote office. This is because the main office LAN is just as trusted as the remote office LAN.
2. The networks associated with the tunnels are added to the existing private zone
3. The protocols for ESP, NAT-T encapsulated IPSec, and ISAKMP are defined in the “application” list, so that specific rules for the encrypted traffic can then be created.
4. Rules are created to allow IPSec, ISAKMP, and NAT-T-encapsulated IPSec out to the Internet.

```
Remote(config)#zone private
Remote(config-zone)#network Main_Office
Remote(config-network)#ip subnet 10.10.10.0/24
Remote(config-network)#exit
Remote(config-zone)#exit
Remote(config-zone)#network tunnel1
Remote(config-network)#ip subnet 10.0.0.0/30
Remote(config-network)#exit
Remote(config-zone)#exit
Remote(config-zone)#network tunnel2
Remote(config-network)#ip subnet 10.0.0.4/30
Remote(config-network)#exit
Remote(config-zone)#exit
Remote(config)#application esp
Remote(config-application)#protocol 50
Remote(config-application)#exit
Remote(config)#application ipsec_nat_t
Remote(config-application)#protocol udp
Remote(config-application)#sport 4500
Remote(config-application)#dport 4500
Remote(config-application)#exit
Remote(config)#application isakmp
Remote(config-application)#protocol udp
Remote(config-application)#sport 500
Remote(config-application)#dport 500
Remote(config-application)#exit
Remote(config)#firewall
Remote(config-firewall)#rule 30 permit esp from public.wan.router to
public
Remote(config-firewall)#rule 40 permit isakmp from public.wan.router to
public
Remote(config-firewall)#rule 50 permit ipsec_nat_t from
public.wan.router to public
Remote(config-firewall)#exit
```

### IP route configuration

The primary route to the main office LAN subnet is configured over the tunnel on eth1.

```
Remote(config)#ip route 10.10.10.0/24 tunnel1
Remote(config)#exit
```

## Failover and scripts

To configure failover we need to configure some ping polls, some triggers, and some scripts.

Create a file called tunnel_1_down.scp, which brings up the backup tunnel, and moves the route to the main office LAN over to that tunnel. The content of the file is:

```
ena
con t
int tunnel2
no shut
ex
ip route 10.10.10.0/24 tunnel2
no ip route 10.10.10.0/24 tunnel1
```

Create a file called tunnel_1_up.scp, which takes down the backup tunnel, and moves the route to the main office LAN back to the primary tunnel.

The content of the file is:

```
ena
con t
int tunnel2
shut
ex
no ip route 10.10.10.0/24 tunnel2
ip route 10.10.10.0/24 tunnel1
```

Ping Poll needs to be configured on the firewall. The ping-poll sends pings to the IP address of the far end of the primary tunnel. If the pings fail, then a ping-poll down trigger will go off. Then when the pings start to succeed again, a ping-poll up trigger will go off.

The required configuration is:

```
Remote#configure terminal
Remote(config)#ping-poll 1
Remote(config-ping-poll)#ip 10.0.0.1
Remote(config-ping-poll)#normal-interval 1
Remote(config-ping-poll)#up-count 3
Remote(config-ping-poll)#fail-count 3
Remote(config-ping-poll)#active
Remote(config-ping-poll)#exit
```

Lastly, set up the triggers so that when pings to the far end of the primary tunnel fail, the backup tunnel becomes active, and then when the pings succeed again, the VPN traffic is moved back to the primary tunnel.

The required configuration is:

```
Remote(config)#trigger 1
Remote(config-trigger)#type ping-poll 1 down
Remote(config-trigger)#script 1 tunnel_1_down.scp
Remote(config-trigger)#exit
Remote(config)#trigger 2
Remote(config-trigger)#type ping-poll 1 up
Remote(config-trigger)#script 1 tunnel_1_up.scp
Remote(config-trigger)#exit
Remote(config)#exit
Remote#write
```

# Remote OpenVPN Client Access

To enable a more flexible working environment, remote users can securely access the main office LAN using an OpenVPN client.

The steps required to enable this secure roaming connection are:

- RADIUS and user configuration
- Some changes to network and firewall configuration
- Certificate generation
- Client configuration

### RADIUS server and user configuration

The AR-Series Firewall router can operate as the RADIUS server to authenticate the OpenVPN connections, and the router can be configured as the local CA (Certificate Authority) trust point.

Note that the RADIUS server needs to be configured with a separate Group for the user of each incoming OpenVPN client connection, and the user needs to be added to the local RADIUS user database.

```
Main_Office(config)#radius-server host 127.0.0.1 key radius
Main_Office(config)#aaa authentication openvpn default group radius
Main_Office(config)#crypto pki trustpoint local
Main_Office(config)#radius-server local
Main_Office(config-radsrv)#server enable
Main_Office(config-radsrv)#nas 127.0.0.1 key radius
Main_Office(config-radsrv)#group client1
Main_Office(config-radsrv-group)#attribute Framed-IP-Address
192.168.250.254
Main_Office(config-radsrv-group)#attribute Framed-IP-Netmask
255.255.255.0
Main_Office(config-radsrv-group)#attribute Framed-Route "10.10.10.0/24
192.168.250.1"
Main_Office(config-radsrv-group)#exit
Main_Office(config-radsrv)#user user1 encrypted password <password1>
group client1
Main_Office(config-radsrv)#exit
```

### Network and firewall configuration

A virtual tunnel interface needs to be added for the OpenVPN connection. The Open VPN application is configured, and the OpenVPN tunnel (tunnel20) is added to the existing private zone. Finally, an allow rule is configured, that permits the incoming OpenVPN traffic (defined by the OpenVPN 'application').

```
Main_Office(config)#interface tunnel20
Main_Office(config-if)#ip address 192.168.250.1/24
Main_Office(config-if)#tunnel openvpn port 1194
Main_Office(config-if)#tunnel mode openvpn tun
Main_Office(config-if)#exit
awplus(config)#application openvpn
awplus(config-application)#protocol udp
awplus(config-application)#dport 1194
Main_Office(config)#zone private
Main_Office(config-zone)#network tunnel20
Main_Office(config-network)#ip subnet 192.168.250.0/24
Main_Office(config-network)#exit
Main_Office(config-zone)#exit
Main_Office(config)#
Main_Office(config)#firewall
Main_Office(config-firewall)#rule 200 permit openvpn from public to
public.wan.router
Main_Office(config-firewall)#exit
Main_Office(config)#
```

## Generating the certificates

In order to connect from the clients, a certificate needs to be generated and exported for the OpenVPN client to use. The commands to obtain a CA certificate from the local Certificate Authority and to export the certificate to a file named cacert.pem, stored in local Flash memory are:

```
Main_Office(config)#crypto pki enroll local
Main_Office(config)#crypto pki export local pem cacert.pem
Main_Office(config)#exit
```

Then copy the cacert.pem file (located in the Root directory in router Flash memory) to distribute to the clients.

## Configuring the client

Install the OpenVPN client application into the client computer. The application can be obtained from the OpenVPN website. Several OpenVPN client apps are available for many platforms.

Most have in common that they rely on a **.ovpn file.** Once the .ovpn file is created, client configuration is typically a matter of loading the file to allow the client device to form a VPN. Samples of .ovpn file templates can also be found on the OpenVPN website. These sample templates typically include explanations of the various .ovpn file configuration options, advice on default settings, and also show locations of where to paste the cacert.pem content.

Each OpenVPN client logs in using a unique user name and password, matching the username configured in the router local RADIUS user database.

Some OpenVPN clients are able to reference the CA certificate file directly, without having to paste in the certificate information into the .ovpn file template as below.

In that case, just place a copy of the certificate file cacert.pem into a directory in the computer.

An Open VPN client can be configured to use the .ovpn sample config file below;

```
remote x.x.x.x 1194 udp
pull
tls-client
cipher AES-128-CBC a
uth SHA1
tls-cipher TLS-DHE-RSA-WITH-AES-256-CBC-SHA
auth-user-pass
ca cacert.pem
dev-type tun topology subnet
port 1194
verb 7
```

Additionally, the **show crypto pki certificates local** command can be used to display the start and end dates of the certificates on the device to ensure they are valid:

```
awplus#show crypto pki certificates local
--------------------
Trustpoint "local" Certificate Chain
--------------------
Self-signed root certificate
  Subject: /O=Allied Telesis, Inc.CN=AlliedWarePlusCAA05050G152000036
  Issuer: /O=Allied Telesis, Inc./CN=AlliedWarePlusCAA05050G152000036
  Valid From: Jun 11 10:41:50 2016 GMT
  Valid To: Jun 9 10:41:50 2026 GMT
  Fingerprint : 5C6A616A 3A28699A D24156E5 505E4CE7 2B109D0D
```

# AMF Node Configuration

This section provides some additional configuration for AMF to use the AR-Series Firewall as an AMF node:

## Adding the AR-Series Firewall to the AMF network

The following configurations is are provided below:

- ATMF network configuration
- Changes to the firewall configuration

The configuration steps below apply to both AR-Series Firewalls.

### AMF network configuration

Host names are used as the node name for AMF nodes and MUST BE UNIQUE within an AMF area. These have been previously configured.

Each AR-Series Firewall needs to be configured with the name of the AMF network they are being added to.

```
Main_Office#
Main_Office#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Main_Office(config)#atmf network name [AMF network name]
```

Configure a switchport as an AMF link that is used to connect to a local AMF master. When the switchport is configured to be an AMF link, it is automatically placed into trunk mode providing access to the default AMF control VLANs (4091 and 4092), and connectivity to the AMF master.

```
Main_Office#
Main_Office#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Main_Office(config)#interface port1.0.1
Main_Office(config-if)#switchport atmf-link
Main_Office(config-if)#exit
```

## Firewall configuration

A firewall zone needs to be created specifically for the AMF subnet, and traffic within that subnet allowed through the firewall.

```
Main_Office(config)#
Main_Office(config)#zone atmf
Main_Office(config-zone)#network management
Main_Office(config-network)#ip subnet 172.31.0.0/17
Main_Office(config-network)#exit
Main_Office(config-zone)#network domain
Main_Office(config-network)#ip subnet 172.31.128.0/17
Main_Office(config-network)#exit
Main_Office(config-zone)#exit
Main_Office(config)#firewall
Main_Office(config-firewall)#rule 300 permit any from atmf to atmf
Main_Office(config-firewall)#exit
Main_Office(config)#exit
Main_Office#write
```

Allied Telesis™ NETWORK SMARTER

**North America Headquarters** | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
**Asia-Pacific Headquarters** | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
**EMEA & CSA Operations** | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

**alliedtelesis**.com

© 2016 Allied Telesis, Inc. All rights reserved. Information in this document is subject to change without notice. All company names, logos, and product designs that are trademarks or registered trademarks are the property of their respective owners.