AlliedWare™ OS

How To | Configure VoIP and Data over a Meshed IPsec VPN

Introduction

This document describes a solution for multiple remote offices requiring a secure VPN connection to a Head Office. This scenario also caters for the following provisions:

- Data needs to be transferred securely from one remote office to another.
- VoIP traffic also needs to be transferred securely between remote offices and the Head Office, and also between remote offices.
- The WAN IP address on the Head Office router is fixed.
- The WAN IP addresses on the Remote Office routers are dynamic—they are allocated by the ISP when the routers bring up their links.
- The IP addresses being used on the LANs at the remote offices are known.

What information will you find in this document?

This document is divided into the following sections:

Which products and software version does this information apply to?

The information provided in this document applies to the following products:

- AR400 Series routers
- AR750S and AR770S routers
- Rapier and Rapier i Series switches
- AT-8800 Series switches

running software version 2.7.1 and above.

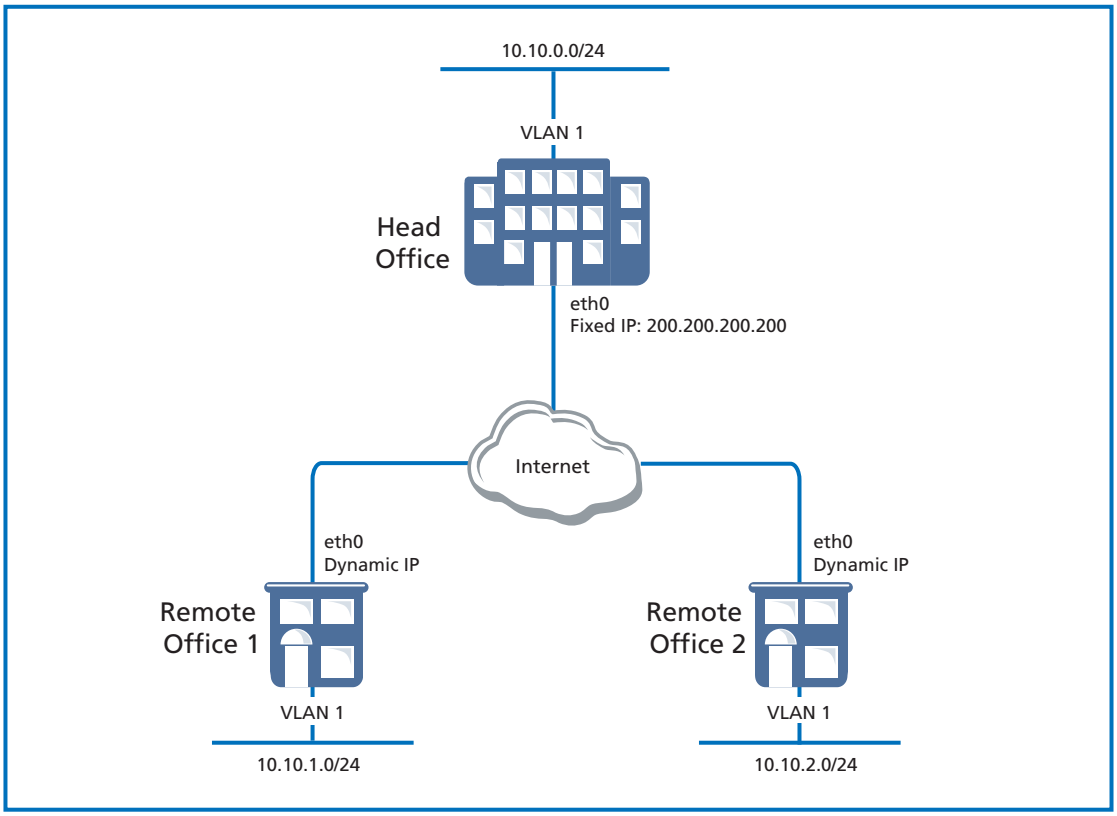
Related How To Notes

Allied Telesis offers How To Notes with a wide range of VPN solutions, from quick and simple solutions for connecting home and remote offices, to advanced multi-feature setups. Notes also describe how to create a VPN between an Allied Telesis router and equipment from a number of other vendors.

For a complete list of VPN How To Notes, see the *Overview of VPN Solutions in How To Notes* in the How To Library at www.alliedtelesis.com/resources/literature/howto.aspx.

Establishing VPN communication between the remote offices and the Head Office

Consider a simplified case, where there are just two remote offices:



The configurations required to establish VPNs between the remote offices and the Head Office are quite straightforward. The key point is that the fixed address on the Head Office WAN interface is the peer address in the ISAKMP and IPsec policies on the remote offices.

Head Office Router

```
set system name="head"
set user securedelay=600
add user=secoff pass=secoff priv=security login=yes

enable ip
add ip int=vlan1 ip=10.10.0.1 mask=255.255.255.0
add ip int=eth0 ip=200.200.200.200
add ip route=0.0.0.0 mask=0.0.0.0 int=eth0 nexthop=200.200.200.201

enable firewall
create firewall policy="nat"
enable firewall policy="nat" icmp_f=all
```

```
add firewall policy="nat" int=vlan1 type=private

add firewall policy="nat" int=eth0 type=public

add firewall policy="nat" nat=enhanced int=vlan1 gblint=eth0

add firewall policy="nat" rule=2 ac=allow int=eth0 prot=udp port=500
  ip=200.200.200.200 gblip=200.200.200.200 gblport=500


# Also, two no-NAT rules are needed: one applied to the public interface
# and one applied to the private interface. This way the office-to-
# office payload traffic will bypass NAT regardless of which end
# initiated the session.

# The rule for the public interface uses encapsulation=ipsec to
# identify incoming VPN traffic.

add firewall policy="nat" rule=3 act=nonat int=eth0 prot=ALL
  ip=10.10.0.1-10.10.255.254 encap=ipsec

# The rule for the private interface uses source and destination
# addresses to identify outgoing VPN traffic.

add firewall policy="nat" rule=4 act=nonat int=vlan1 prot=ALL
  ip=10.10.0.1-10.10.255.254 remoteip=10.10.0.1-10.10.255.254


create ipsec saspec=1 key=isakmp protocol=esp encalg=des
  hashalg=null

create ipsec bundle=1 key=isakmp string="1"

create ipsec policy="isa" int=eth0 act=permit

set ipsec policy="isa" lport=500 rport=500


create ipsec policy="rem1" int=eth0 act=ipsec key=isakmp bundle=1

     peer=DYNAMIC

set ipsec policy="rem1" laddress=10.10.0.0 lmask=255.255.0.0
  raddress=10.10.1.0 rmask=255.255.255.0


create ipsec policy="rem2" int=eth0 act=ipsec key=isakmp bundle=1
  peer=DYNAMIC

set ipsec policy="rem2" laddress=10.10.0.0 lmask=255.255.0.0
  raddress=10.10.2.0 rmask=255.255.255.0


create ipsec policy="internet" int=eth0 act=permit

enable ipsec


create enco key=1 value=testkey type=general

create isakmp policy="dyn" peer=any key=1

enable isakmp
```

Remote Office 1 Router

```
set system name="Remote-1"
set user securedelay=600
add user=secoff pass=secoff priv=security login=yes

enable ip
enable ip remote
add ip int=vlan1 ip=10.10.1.1 mask=255.255.255.0
add ip int=eth0 ip=dhcp

enable firewall
create firewall policy="nat"
enable firewall policy="nat" icmp_f=all
add firewall policy="nat" int=vlan1 type=private
add firewall policy="nat" int=eth0 type=public
add firewall policy="nat" nat=enhanced int=vlan1 gblint=eth0

add firewall policy="nat" rule=1 act=allow int=eth0 prot=udp
  port=500 ip=10.10.1.1 gblip=0.0.0.0 gblport=500
add firewall policy="nat" rule=2 act=nonat int=eth0 prot=ALL
  ip=10.10.0.1-10.10.255.254 encap=ipsec
add firewall policy="nat" rule=10 ac=nonat int=vlan1 prot=ALL
  ip=10.10.0.1-10.10.255.254 remoteip=10.10.0.1-10.10.255.254

create ipsec saspec=1 key=isakmp prot=esp encalg=des hashalg=null
create ipsec bundle=1 key=isakmp string="1"
create ipsec policy="isa" int=eth0 act=permit
set ipsec policy="isa" lport=500 rport=500

create ipsec policy="head" int=eth0 act=ipsec key=isakmp bundle=1
  peer=200.200.200.200
set ipsec policy="head" laddress=10.10.1.0 lmask=255.255.255.0
  raddress=10.10.0.0 rmask=255.255.0.0

create ipsec policy="internet" int=eth0 act=permit
enable ipsec

create enco key=1 value=testkey type=general
create isakmp policy="dyn" peer=200.200.200.200 key=1
enable isakmp
```

Remote Office 2 Router

```
set system name="Remote-2"
set user securedelay=600
add user=secoff pass=secoff priv=security login=yes

enable ip
enable ip remote
add ip int=vlan1 ip=10.10.2.1 mask=255.255.255.0
add ip int=eth0 ip=dhcp

enable firewall
create firewall policy="nat"
enable firewall policy="nat" icmp_f=all
add firewall policy="nat" int=vlan1 type=private
add firewall policy="nat" int=eth0 type=public
add firewall policy="nat" nat=enhanced int=vlan1 gblint=eth0

add firewall policy="nat" rule=1 act=allow int=eth0 prot=udp
  port=500 ip=10.10.2.1 gblip=0.0.0.0 gblport=500
add firewall policy="nat" rule=2 act=nonat int=eth0 prot=ALL
  ip=10.10.0.1-10.10.255.254 encap=ipsec
add firewall policy="nat" rule=10 ac=nonat int=vlan1 prot=ALL
  ip=10.10.0.1-10.10.255.254 remoteip=10.10.0.1-10.10.255.254

create ipsec saspec=1 key=isakmp prot=esp encalg=des hashalg=null
create ipsec bundle=1 key=isakmp string="1"
create ipsec policy="isa" int=eth0 act=permit
set ipsec policy="isa" lport=500 rport=500

create ipsec policy="head" int=eth0 act=ipsec key=isakmp bundle=1
  peer=200.200.200.200
set ipsec policy="head" laddress=10.10.2.0 lmask=255.255.255.0
  raddress=10.10.0.0 rmask=255.255.0.0

create ipsec policy="internet" int=eth0 act=permit
enable ipsec
create enco key=1 value=testkey type=general
create isakmp policy="dyn" peer=200.200.200.200 key=1
enable isakmp
```

The main challenge: routing VPN traffic from one remote office to another

It can be difficult to route between two remote offices when they both have dynamic IP addresses. The only practical way to achieve communication between two remote offices is to have them communicate to each other via the Head Office router.

But, the great thing is that the configuration given above achieves this with no extra configuration—it will also allow VPN traffic to be passed between remote offices.

The key to understanding this is to look at the process by which the routers decide which packets go into the IPsec tunnels. Let us look at the encapsulation decisions made in packet exchanges between different pairs of LANs in the network, with the configuration above.

Encapsulation decisions

Remote Office 1 will open an IPsec tunnel to Head Office and encapsulate every packet that wants to go from 10.10.1.0/24 to 10.10.0.0/16 with IPsec, according to the configured IPsec policy named "head". The rest of the traffic, which does not match to the "head" policy, will be sent unencrypted to the Internet. Please note that the remote address range for the "head" policy is not just the LAN address range of Head Office (10.10.0.0/24), but, instead, includes all the local address ranges of the other remote offices (10.10.0.0/16). We will see below that this is a key part of the solution for enabling the remote offices to communicate to each other over the VPN.

Remote Office 2 will open an IPsec tunnel to Head Office and encapsulate every packet that wants to go from 10.10.2.0/24 to 10.10.0.0/16 with IPsec, according to the configured IPsec policy named "head". The rest of the traffic, which does not match to the "head" policy, will be sent unencrypted to the Internet. Again, the remote address range for "head" policy, is 10.10.0.0.

- The Head Office learns the dynamic WAN IP addresses of Remote Office 1 and Remote Office 2 while opening the tunnels to the remote offices. And while the tunnels are being opened, the Head Office router learns the LAN addresses of Remote Office 1 and Remote Office 2, as the local address (**laddress**) and remote address (**raddress**) parameters are negotiated during the IPsec SA negotiation.
- When Head Office wants to send data to Remote Office 1's LAN, it checks the IPsec policies it has, and sends the packet through the tunnel that has the matching local and remote addresses.
- When Remote Office 1 wants to send a packet to Remote Office 2, it looks up its IPsec policy table and finds that a packet from 10.10.1.x to 10.10.2.x matches to the policy "head", so it sends the packet to Head Office WAN IP address with the negotiated encapsulation and encryption.
- Then Head Office router receives the packet and decrypts it. After decryption, it checks the inner part of the packet to see where packet is going to. It reads that the destination IP is 10.10.2.x and that the packet originated from 10.10.1.x. It checks its routing table, and does not find a specific route for 10.10.2.x, so sends it to its default route, out of interface eth0.

  When it sends the packet out, the Head Office router checks which IPsec policy the packet matches. When the router tries to match the packet to a policy, it reads its policy table, step-by-step, and it figures out that a packet from 10.10.1.x to 10.10.2.x matches the policy "rem2". Therefore, it sends the packet down the tunnel to Remote Office 2.

Configuring the VoIP PIC

The AR027 2-port VoIP FXS PIC card can be installed into AR410, AR44x, AR725, AR745 and Rapier i products. With the AR027 module installed, these products provide a one-box VoIP and VPN solution. Once the VoIP PIC has been installed, the configuration required to set the router (or switch) up to act as a SIP endpoint is:

```
set voip boot=c-1-0-0.bin server=flash

set voip pub int=eth0

set voip file=ss-1-0-0.bin protocol=sip type=fxs

ena voip protocol=sip engine=fxs0

cre sip int=fxs0.0 phone=201 domain=10.10.0.2 proxy=10.10.0.2
  location=10.10.0.2 capablity=g723r53 username=<name>
  password=<password>

cre sip int=fxs0.1 phone=202 domain=10.10.0.2 proxy=10.10.0.2
  location=10.10.0.2 capability=g723r53 username=<name>
  password=<password>
```

The equivalent configuration to set the PIC up for H.323 is:

```
set voip boot=c-1-0-0.bin server=flash

set voip pub int=eth0

set voip file=hs-1-0-0.bin protocol=h323 type=fxs

ena voip protocol=h323 engine=fxs0

set h323 gate gatekeeper=10.10.0.2

cre h323 int=fxs0.0 phone=201 capablity=g723r53

cre h323 int= fxs0.1 phone=202 capability=g723r53
```

Note: The files c-1-0-0.bin, hs-1-0-0.bin, and ss-1-0-0.bin must be loaded into the router or switch's Flash memory for VoIP to operate. These files can be downloaded from the PIC's product area at www.alliedtelesis.com/products/detail.aspx?pid=139&lid=38.

Using software QoS to prioritize VoIP traffic

A DAR (Dynamic Application Recognition) entity can be used to recognise VoIP sessions, and give the VoIP payload traffic second-top priority. The VoIP signalling traffic can be given top priority.

An example of how to configure this in the case when VoIP PIC is running SIP would be as follows:

```
create classifier=1 udpdport=5060

enable sqos
create sqos dar=1 protocol=SIP
create sqos trafficclass=1 priority=15
create sqos trafficclass=2 priority=14 maxqlen=10
create sqos policy=1
add sqos policy=1 trafficclass=1,2
add sqos trafficclass=1 classifier=1
add sqos trafficclass=2 dar=1
set sqos interface=ipsec-head tunnelpolicy=1
add sqos interface=ipsec-head dar=1
```

Note that the software QoS policy is applied to the IPSec tunnel "interface". So, it gives relative priority to different traffic types as they enter the tunnel.

To check that the DAR is actually detecting VoIP sessions, you can use the command **show sqos counter dar**:

```
Manager ar440_FW> show sqos count dar
DAR Object 1
-------------------------------------------------------------------------
Session Counters (by protocol)
Total Sessions Recognised.. 2
RTSP Sessions Recognised... 0
SIP Sessions Recognised.... 2
H323 Sessions Recognised... 0
Session Counters (by media)
Active Sessions............ 2
Voice Sessions Started..... 2
Video Sessions Started..... 0
Dynamic Classifiers
Classifer=10000 tc=1 ip=192.168.2.2/32 port=50600-50601
Classifer=10001 tc=1 ip=202.49.72.14/32 port=17818-17819
```

USA Headquarters | 19800 North Creek Parkway | Suite 200 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesis.com

C613-16080-00 REV D

Connecting The IP World

Allied Telesis