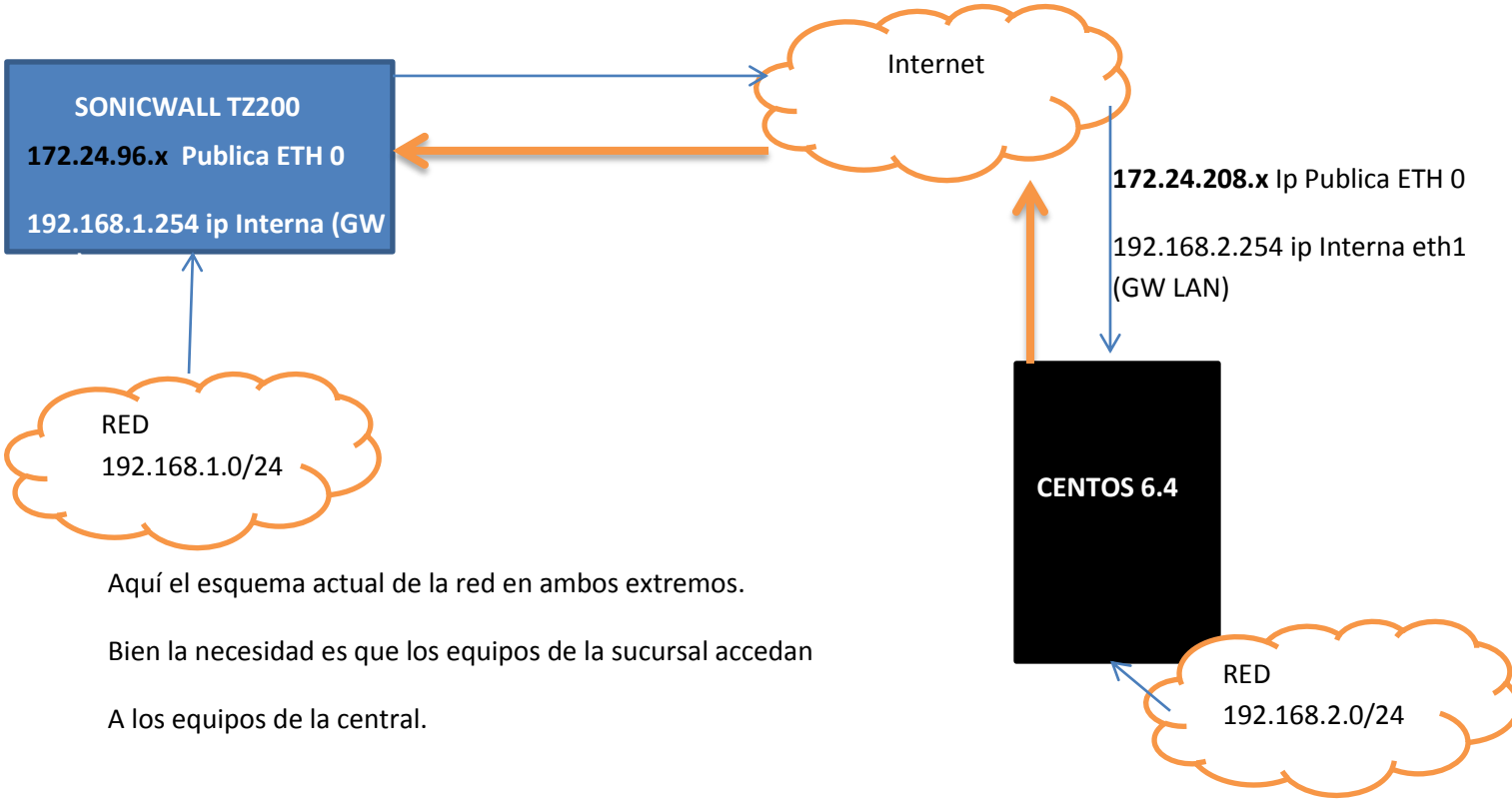
Esquema de Conectividad




Aquí el esquema actual de la red en ambos extremos.

Bien la necesidad es que los equipos de la sucursal accedan

A los equipos de la central.

Datos de Ipsec Sucursal:

```
# /etc/ipsec.conf - Openswan IPsec configuration file
#
# Manual:     ipsec.conf.5
#
# Please place your own config files in /etc/ipsec.d/ ending in .conf


version 2.0     # conforms to second version of ipsec.conf specification


# basic configuration
config setup
        # Debug-logging controls:  "none" for (almost) none, "all" for lots.
```

```
# klipsdebug=none
# plutodebug="control parsing"
# For Red Hat Enterprise Linux and Fedora, leave protostack=netkey
protostack=netkey
interfaces=%defaultroute
nat_traversal=yes
forwardcontrol=yes
virtual_private=%v4:10.0.0.0/8
oe=off
# Enable this if you see "failed to find any available worker"
nhelpers=0
```

**IPTABLES**

```
[root@GWLOMA ~]# service iptables status
Tabla: mangle
Chain PREROUTING (policy ACCEPT)
num  target     prot opt source               destination

Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
```

```
Chain POSTROUTING (policy ACCEPT)
num  target     prot opt source               destination


Tabla: nat
Chain PREROUTING (policy ACCEPT)
num  target     prot opt source               destination
1    DNAT       tcp  --  172.24.96.x        0.0.0.0/0          tcp dpt:3389 to:192.168.2.3:3389


Chain POSTROUTING (policy ACCEPT)
num  target     prot opt source               destination
1    MASQUERADE  all  --  192.168.2.0/24       0.0.0.0/0
2    MASQUERADE  all  --  192.168.2.0/24       0.0.0.0/0


Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination


Tabla: filter
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  0.0.0.0/0           0.0.0.0/0          state RELATED,ESTABLISHED
2    ACCEPT     icmp --  0.0.0.0/0           0.0.0.0/0
3    ACCEPT     all  --  0.0.0.0/0           0.0.0.0/0
4    ACCEPT     udp  --  0.0.0.0/0           0.0.0.0/0          udp spt:5353
5    ACCEPT     udp  --  0.0.0.0/0           0.0.0.0/0          udp spt:427
6    ACCEPT     tcp  --  0.0.0.0/0           0.0.0.0/0          state NEW tcp dpt:22
7    ACCEPT     tcp  --  192.168.1.0/24       0.0.0.0/0          tcp dpt:631
```

```
8   ACCEPT    tcp  --  0.0.0.0/0          0.0.0.0/0          tcp dpt:3389
9   ACCEPT    tcp  --  172.24.96.x        0.0.0.0/0
10  ACCEPT    tcp  --  192.168.2.0/24      0.0.0.0/0          tcp dpt:5502
11  ACCEPT    tcp  --  192.168.2.0/24      0.0.0.0/0          tcp dpt:5902
12  ACCEPT    tcp  --  0.0.0.0/0          0.0.0.0/0          tcp dpt:500
13  ACCEPT    udp  --  0.0.0.0/0          0.0.0.0/0          udp dpt:500
14  ACCEPT    udp  --  0.0.0.0/0          0.0.0.0/0          udp dpt:4500
15  ACCEPT    tcp  --  0.0.0.0/0          0.0.0.0/0          tcp dpt:4500
16  ACCEPT    tcp  --  0.0.0.0/0          0.0.0.0/0          tcp dpt:50
17  ACCEPT    esp  --  0.0.0.0/0          0.0.0.0/0
18  ACCEPT    ah   --  0.0.0.0/0          0.0.0.0/0
19  ACCEPT    tcp  --  192.168.2.0/24      0.0.0.0/0          tcp dpt:15000
20  ACCEPT    esp  --  0.0.0.0/0          0.0.0.0/0

Chain FORWARD (policy ACCEPT)
num  target    prot opt source             destination
1   ACCEPT    esp  --  0.0.0.0/0          192.168.2.0
2   ACCEPT    esp  --  192.168.2.0/24      0.0.0.0/0
3   ACCEPT    udp  --  0.0.0.0/0          192.168.2.0/24     udp spt:500 dpt:500
4   ACCEPT    udp  --  192.168.2.0/24      0.0.0.0/0          udp spt:500 dpt:500
5   ACCEPT    udp  --  0.0.0.0/0          192.168.2.0/24     udp spt:4500 dpt:4500
6   ACCEPT    udp  --  192.168.2.0/24      0.0.0.0/0          udp spt:4500 dpt:4500
7   ACCEPT    tcp  --  0.0.0.0/0          192.168.2.0/24     tcp spt:10000 dpt:10000
8   ACCEPT    tcp  --  192.168.2.0/24      0.0.0.0/0          tcp spt:10000
9   ACCEPT    tcp  --  0.0.0.0/0          192.168.2.0/24     tcp spt:10000
10  ACCEPT    ah   --  192.168.2.0/24      0.0.0.0/24
```

```
11   ACCEPT     ah   --  0.0.0.0/0          192.168.2.0/24


Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     esp  --  0.0.0.0/0          0.0.0.0/0
Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
```

**CONF p/ SONICWALL**

```
 [root@GWLOMA ~]# cat /etc/ipsec.d/central.conf
conn central
        type=tunnel
        auto=add
        aggrmode=no
        forceencaps=yes
        # ikelifetime=28800
        # keylife=5h
        ike=3des-md5-modp1024
        esp=3des-md5
        authby=secret
         #keyexchange=ike
        keyingtries=1
        pfs=no
        auth=esp
        left=172.24.208.x
        leftnexthop=%defaultroute
        leftsubnet=192.168.2.0/24
```

```
        leftid=172.24.208.x
        leftxauthclient=no
        right=172.24.96.x
        rightnexthop=%defaultroute
        rightsubnet=192.168.1.0/24
        rightid=172.24.96.x
        rightxauthserver=no
[root@GWLOMA ~]#
```

**[root@GWLOMA ~]# ipsec verify**

```
Checking your system to see if IPsec got installed and started correctly:
Version check and ipsec on-path                         [OK]
Linux Openswan U2.6.29/K2.6.32.26-175.fc12.x86_64 (netkey)
Checking for IPsec support in kernel                    [OK]
NETKEY detected, testing for disabled ICMP send_redirects      [OK]
NETKEY detected, testing for disabled ICMP accept_redirects    [OK]
Checking that pluto is running                          [OK]
Pluto listening for IKE on udp 500                      [OK]
Pluto listening for NAT-T on udp 4500                   [OK]
Two or more interfaces found, checking IP forwarding          [OK]
Checking NAT and MASQUERADEing                          [N/A]
Checking for 'ip' command                               [OK]
Checking for 'iptables' command                         [OK]
Opportunistic Encryption Support                        [DISABLED]
[root@GWLOMA ~]#
```

**[root@GWLOMA ~]# ipsec auto --up central**

**104 "central" #1: STATE_MAIN_I1: initiate**

**003 "central" #1: ignoring unknown Vendor ID payload [5b362bc820f60007]**

**003 "central" #1: received Vendor ID payload [RFC 3947] method set to=109**

**106 "central" #1: STATE_MAIN_I2: sent MI2, expecting MR2**

**003 "central" #1: ignoring Vendor ID payload [Sonicwall 1 (TZ 170 Standard?)]**

**003 "central" #1: received Vendor ID payload [XAUTH]**

**003 "central" #1: received Vendor ID payload [Dead Peer Detection]**

**003 "central" #1: NAT-Traversal: Result using RFC 3947 (NAT-Traversal): both are NATed**

**108 "central" #1: STATE_MAIN_I3: sent MI3, expecting MR3**

**003 "central" #1: ignoring informational payload, type IPSEC_INITIAL_CONTACT msgid=00000000**

**004 "central" #1: STATE_MAIN_I4: ISAKMP SA established {auth=OAKLEY_PRESHARED_KEY cipher=oakley_3des_cbc_192 prf=oakley_md5 group=modp1024}**

**117 "central" #2: STATE_QUICK_I1: initiate**

**004 "central" #2: STATE_QUICK_I2: sent QI2, IPsec SA established tunnel mode {ESP/NAT=>0x79ed9e8f <0xa37c8943 xfrm=3DES_0-HMAC_MD5 NATOA=none NATD=172.24.96.x:4500 DPD=none}**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 3 | VPN Loma | 172.24.208[redacted] | | 192.168.2.0 - 192.168.2.255 | ESP: 3DES/HMAC MD5 (IKE) | | |

---

Tunel Establecido.

<u>En el Linux:</u>

[root@GWLOMA ~]# route -n

Kernel IP routing table

| Destination | Gateway | Genmask | Flags | Metric | Ref | Use | Iface |
|---|---|---|---|---|---|---|---|
| 172.24.208.x | 0.0.0.0 | 255.255.255.252 | U | 0 | 0 | 0 | eth0 |
| 192.168.2.0 | 0.0.0.0 | 255.255.255.0 | U | 0 | 0 | 0 | eth1 |
| 169.254.0.0 | 0.0.0.0 | 255.255.0.0 | U | 1002 | 0 | 0 | eth1 |

169.254.0.0 0.0.0.0 255.255.0.0 U 1003 0 0 eth0

0.0.0.0 172.24.208.x 0.0.0.0 UG 0 0 0 eth0

**[root@GWLOMA ~]# ping 172.24.96.x**

PING 172.24.96.30 (172.24.96.30) 56(84) bytes of data.

64 bytes from 172.24.96.x: icmp_seq=1 ttl=60 time=1.99 ms

64 bytes from 172.24.96.x: icmp_seq=2 ttl=60 time=1.87 ms

64 bytes from 172.24.96.x: icmp_seq=3 ttl=60 time=1.94 ms

64 bytes from 172.24.96.x: icmp_seq=4 ttl=60 time=1.77 ms

64 bytes from 172.24.96.x: icmp_seq=5 ttl=60 time=1.79 ms

64 bytes from 172.24.96.x: icmp_seq=6 ttl=60 time=1.73 ms

64 bytes from 172.24.96.x: icmp_seq=7 ttl=60 time=1.82 ms

64 bytes from 172.24.96.x: icmp_seq=8 ttl=60 time=1.88 ms

64 bytes from 172.24.96.x icmp_seq=9 ttl=60 time=1.79 ms

^C

--- 172.24.96.30 ping statistics ---

9 packets transmitted, 9 received, 0% packet loss, time 8500ms

rtt min/avg/max/mdev = 1.737/1.848/1.996/0.080 ms

[root@GWLOMA ~]#

**El Linux ve al ip accesible de la VPN**

**Y en el Sonicwall**

**Currently Active VPN Tunnels**

Refresh Interval (secs) 10 Items per page 50

| # | Created | Name | Local | Remote | Gateway | |
|---|---|---|---|---|---|---|
| 1 | 05/03/2014 09:56:04 | VPN Loma | 192.168.1.0 - 192.168.1.255 | 192.168.2.0 - 192.168.2.255 | 172.24.208.[redacted] | Re |

1 Currently Active VPN Tunnels