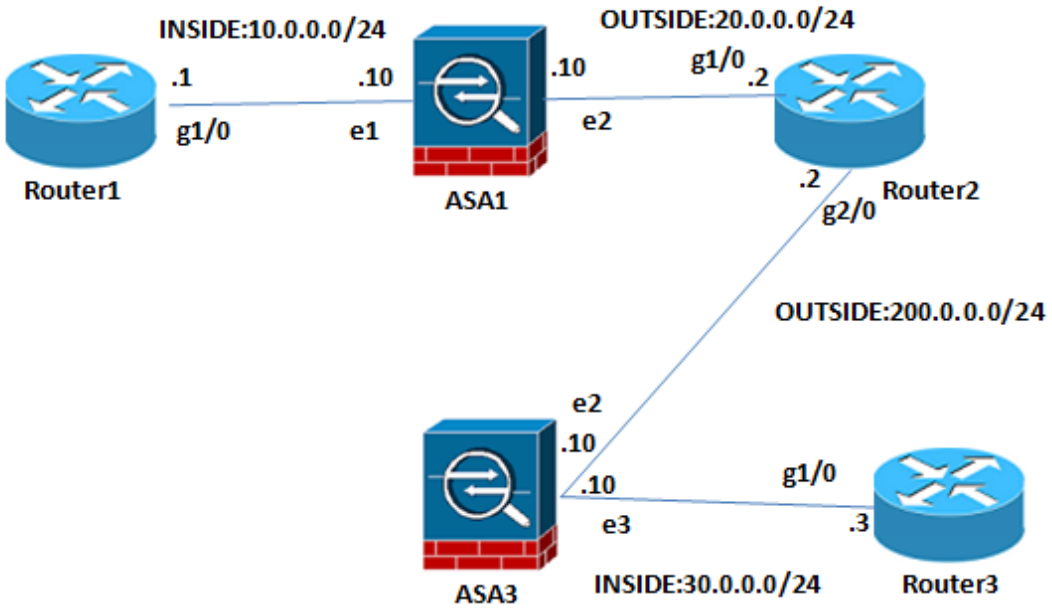
ASA LAN to LAN IPSec configuration

Platform: https://racks.uninets.com
Lab Name: CCIE Security

Topology

ASA LAN to LAN IPSec configuration



Task

- The traffic from R1 Lo0 to R3 should be encrypted. Create IPSec tunnel between R1 and ASA3.
- First make sure that R1 and ASA3 are reachable to each other and routing is fine for the interesting traffic.

Explanation

Like in IOS, ISAKMP Policy defines Phase 1

– Authentication, Hash, Encryption, DH Group
– Like in IOS, processed top down until a match occurs

Like in IOS, Crypto-Map defines Phase 2

– Who? - Peer address
– What? - Proxy ACL
– How? - Transform Set

In IOS, ISAKMP is by default enabled on all interfaces

– On ASA it needs to be manually enabled ---#crypto ikev1 enable outside

ASA Tunnel-Groups

Similar to ISAKMP profiles in IOS

- AKA Connection Profiles
- tunnel-group <name> type [ipsec-l2l|remote-access]
- tunnel-group <name> general-attributes
- tunnel-group <name> [ipsec-attributes|webvpn-attributes]

Matches remote endpoint IKEv1 identity; Address, hostname, certificate, etc.

Defines settings before IPsec session is established

- ISAKMP PSK
- CA Trustpoint
- AAA settings
- IP addressing for remote-access VPN
- Group Policy

ASA Group-Policies

Defines authorization once IPsec is established

- Perfect Forward Secrecy (PFS)
- Split Tunneling
- VPN Filters
- Tunneling Protocols
- E.g. IKEv1, IKEv2, L2TP, SSLVPN (client/clientless)
- DHCP, DNS, Proxy Server, VLAN, NAC, etc.

Can be configured locally or attributes received via RADIUS/LDAP

- group-policy <name> [internal|external]
- group-policy <name> attributes

Mostly relevant for Remote Access VPNs

- Mandatory for all VPN sessions on the ASA

UniNets Document

Helpful command for vpn….

- Vpnsetup
- Show run all tunnel-group / group-policy

When connection comes on ASA, it should land on correct tunnel; it's based on the IKE ID which is generally the IP address of the peer.

Inheritance in ASA

Tunnel of type ipsec-l2l

- Inherits settings from DefaultL2LGroup
- Changes into DefaultL2LGroup are NOT reflected to userconfiguredtunnel-groups

Tunnel of type ipsec-ra

- Inherits settings from DefaultRAGroup
- Changes into DefaultRAGroup are NOT reflected to userconfiguredtunnel-groups

Tunnel of type webvpn

- Inherits settings from DefaultWEBVPNGroup
- Changes into DefaultWEBVPNGroup are NOT reflected to userconfiguredtunnel-groups

There are multiple default tunnel-groups based on the type of tunnels but there is a single default group-policy.

Default tunnel groups acts like a configuration template for userconfiguredtunnel-groups

- However, can be used for active connections; Because of this, changes are not replicated to user-configured tunnel-groups

All tunnel-groups use the same set of authorization attributes by default

- Applies settings from DfltGrpPolicy group-policy

User-configured group-policies

- Can be attached to specific tunnel-groups
- Inherit settings from DfltGrpPolicy
- Changes into DfltGrpPolicy are reflected to user-configured grouppolicies
- User-configured group-policies settings override settings inherited fromDfltGrpPolicy

UniNets Document

Solution

```
R1(config)#ip route 200.0.0.0 255.255.255.0 10.0.0.10

ASA1(config)# route outside 200.0.0.0 255.255.255.0 20.0.0.2

Return traffic

R2#sh run | in ip route

ip route 10.0.0.0 255.255.255.0 20.0.0.10

ASA3(config)# route outside 10.0.0.0 255.255.255.0 200.0.0.2

ASA3(config)# route inside 3.3.3.3 255.255.255.255 30.0.0.3

R3(config)#ip route 0.0.0.0 0.0.0.0 30.0.0.10
```

Temporarily allow ICMP on both ASA for checking connectivity between R1 and ASA3.
(Apply access-list for ICMP on ASA1 is enough)

ASA1

access-list OUTSIDE_IN extended permit icmp any any----- for echo-reply to R1's echo and echo request from ASA3 access-group OUTSIDE_IN in interface outside

```
R1#ping 200.0.0.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/75/112 ms
```

```
ASA3# ping 10.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/122/270 ms
```

Routing for the interesting traffic, these routes should only be present on the IPsec peer devices which determines the outgoing interface via routing and IPsec traffic will initiated.

```
ASA3(config)# route outside 1.1.1.1 255.255.255.255 200.0.0.2
R1(config)#ip route 30.0.0.0 255.255.255.0 g1/0
R1(config)#ip route 3.3.3.3 255.255.255.255 g1/0
```

Make sure the UDP is inspected on ASA1 for Phase-1 and ESP is either inspected or allowed on the outside interface for the peer IP addresses. UDP is inspected by default

```
ASA1# shrun access-list
access-list OUTSIDE_IN extended permit esp host 200.0.0.10 host 10.0.0.1
```

Phase-1

R1

```
cryptoisakmp policy 20
authentication pre-share
encr des
hashsha
group 2
```

ASA3

```
crypto ikev1 policy 10
authentication pre-share
encryption des
hashsha
group 2
lifetime 86400
```

- this is default on ASA and it does not matter because they negotiate to a lower value

```
R1(config)#crypto isakmp key 0 cisco address 200.0.0.10
ASA3(config)# sh run tunnel-group
tunnel-group 10.0.0.1 type ipsec-l2l
tunnel-group 10.0.0.1 ipsec-attributes
ikev1 pre-shared-key *****
```

Phase-2

R1

```
ip access-list extended R1-ASA3
permitip host 1.1.1.1 30.0.0.0 0.0.0.255
permitip host 1.1.1.1 host 3.3.3.3

ASA3
access-list ASA3-R1 extended permit ip 30.0.0.0 255.255.255.0 host 1.1.1.1
access-list ASA3-R1 extended permit ip host 3.3.3.3 host 1.1.1.1
```

R1

```
R1(config)#crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
```

ASA3

```
cryptoipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
```

R1

```
crypto map CRYPTO 20 ipsec-isakmp
set peer 200.0.0.10
set transform-set ESP-DES-SHA
match address R1-ASA3

interface GigabitEthernet1/0
crypto map CRYPTO
```

ASA3

```
crypto map CRYPTO 10 match address ASA3-R1
crypto map CRYPTO 10 set peer 10.0.0.1
crypto map CRYPTO 10 set ikev1 transform-set ESP-DES-SHA

crypto map CRYPTO interface outside  ---apply crypto map
crypto ikev1 enable outside
```

----need to enable it on the interface, it's enabled by default on all interfaces in IOS but not in ASA

```
R1#ping 3.3.3.3 source lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 76/101/144 ms
```

```
R1#ping 30.0.0.3 source lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.0.0.3, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 72/97/116 ms
```

```
R1#sh crypto isakmpsa
IPv4 Crypto ISAKMP SA
dstsrc          state        conn-id slot status
200.0.0.10      10.0.0.1       QM_IDLE          1008    0 ACTIVE

IPv6 Crypto ISAKMP SA
```

```
ASA3# sh crypto isakmpsa

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 10.0.0.1
    Type    : L2L           Role    : responder
    Rekey   : no            State   : MM_ACTIVE

There are no IKEv2 SAs
```

```
R1#sh crypto ipsecsa

protectedvrf: (none)
local  ident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/0/0)
remoteident (addr/mask/prot/port): (3.3.3.3/255.255.255.255/0/0)
current_peer 200.0.0.10 port 500
     PERMIT, flags={origin_is_acl,}
    #pktsencaps: 29, #pkts encrypt: 29, #pkts digest: 29
    #pktsdecaps: 10, #pkts decrypt: 10, #pkts verify: 10
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pktscompr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

local crypto endpt.: 10.0.0.1, remote crypto endpt.: 200.0.0.10
```

```
pathmtu 1500, ipmtu 1500, ipmtuidb GigabitEthernet1/0
current outbound spi: 0xFE509770(4266694512)

inboundespsas:
spi: 0x19730A3C(426969660)
transform: esp-des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 9, flow_id: SW:9, crypto map: CRYPTO
sa timing: remaining key lifetime (k/sec): (4568451/3037)
        IV size: 8 bytes
replay detection support: Y
        Status: ACTIVE

inbound ah sas:

inboundpcpsas:

outboundespsas:
spi: 0xFE509770(4266694512)
transform: esp-des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 10, flow_id: SW:10, crypto map: CRYPTO
sa timing: remaining key lifetime (k/sec): (4568448/3037)
        IV size: 8 bytes
replay detection support: Y
        Status: ACTIVE

outbound ah sas:

outboundpcpsas:

protectedvrf: (none)
local  ident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/0/0)
remoteident (addr/mask/prot/port): (30.0.0.0/255.255.255.0/0/0)
current_peer 200.0.0.10 port 500
     PERMIT, flags={origin_is_acl,}
#pktsencaps: 4, #pkts encrypt: 4, #pkts digest: 4
    #pktsdecaps: 4, #pkts decrypt: 4, #pkts verify: 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pktscompr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

local crypto endpt.: 10.0.0.1, remote crypto endpt.: 200.0.0.10
pathmtu 1500, ipmtu 1500, ipmtuidb GigabitEthernet1/0
current outbound spi: 0xA185B303(2709893891)

inboundespsas:
```

```
spi: 0x2DBF0CA(47968458)
transform: esp-des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 11, flow_id: SW:11, crypto map: CRYPTO
sa timing: remaining key lifetime (k/sec): (4594305/3445)
        IV size: 8 bytes
replay detection support: Y
        Status: ACTIVE

inbound ah sas:

inboundpcpsas:

outboundespsas:
spi: 0xA185B303(2709893891)
transform: esp-des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 12, flow_id: SW:12, crypto map: CRYPTO
sa timing: remaining key lifetime (k/sec): (4594305/3445)
        IV size: 8 bytes
replay detection support: Y
        Status: ACTIVE

outbound ah sas:

outboundpcpsas:
```

```
ASA3# sh crypto ipsecsa
interface: outside
    Crypto map tag: CRYPTO, seqnum: 10, local addr: 200.0.0.10

access-list ASA3-R1 extended permit ip host 3.3.3.3 host 1.1.1.1
localident (addr/mask/prot/port): (3.3.3.3/255.255.255.255/0/0)
remoteident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/0/0)
current_peer: 10.0.0.1

#pktsencaps: 10, #pkts encrypt: 10, #pkts digest: 10
      #pktsdecaps: 29, #pkts decrypt: 29, #pkts verify: 29
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 10, #pkts comp failed: 0, #pktsdecomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulatedfrgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

local crypto endpt.: 200.0.0.10/0, remote crypto endpt.: 10.0.0.1/0
pathmtu 1500, ipsec overhead 58, media mtu 1500
```

```
current outbound spi: 19730A3C
current inbound spi : FE509770

inboundespsas:
spi: 0xFE509770 (4266694512)
transform: esp-des esp-sha-hmac no compression
in use settings ={L2L, Tunnel, }
slot: 0, conn_id: 4096, crypto-map: CRYPTO
sa timing: remaining key lifetime (kB/sec): (4373997/2907)
        IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
         0x00000000 0x3FFFFFFF
outboundespsas:
spi: 0x19730A3C (426969660)
transform: esp-des esp-sha-hmac no compression
in use settings ={L2L, Tunnel, }
slot: 0, conn_id: 4096, crypto-map: CRYPTO
sa timing: remaining key lifetime (kB/sec): (4373999/2905)
        IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
         0x00000000 0x00000001

    Crypto map tag: CRYPTO, seqnum: 10, local addr: 200.0.0.10

access-list ASA3-R1 extended permit ip 30.0.0.0 255.255.255.0 host 1.1.1.1
localident (addr/mask/prot/port): (30.0.0.0/255.255.255.0/0/0)
remoteident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/0/0)
current_peer: 10.0.0.1

#pktsencaps: 4, #pkts encrypt: 4, #pkts digest: 4
      #pktsdecaps: 4, #pkts decrypt: 4, #pkts verify: 4
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 4, #pkts comp failed: 0, #pktsdecomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulatedfrgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

local crypto endpt.: 200.0.0.10/0, remote crypto endpt.: 10.0.0.1/0
pathmtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: 02DBF0CA
current inbound spi : A185B303

inboundespsas:
spi: 0xA185B303 (2709893891)
transform: esp-des esp-sha-hmac no compression
in use settings ={L2L, Tunnel, }
```

```
slot: 0, conn_id: 4096, crypto-map: CRYPTO
sa timing: remaining key lifetime (kB/sec): (4373999/3304)
        IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
         0x00000000 0x0000001F
outboundespsas:
spi: 0x02DBF0CA (47968458)
transform: esp-des esp-sha-hmac no compression
in use settings ={L2L, Tunnel, }
slot: 0, conn_id: 4096, crypto-map: CRYPTO
sa timing: remaining key lifetime (kB/sec): (4373999/3304)
        IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
         0x00000000 0x00000001
```

Note: - Tunnel-group is considered as security level 100 that is the reason the traffic from outside on ASA3 can reach to R3. “sysopt connection permit-vpn” is the default command on ASA. If we remove this command from the ASA3, the traffic from R1’s Lo0 will get dropped on ASA3 outside interface as it is coming from low security level to high security level.

```
ASA3(config)# no sysopt connection permit-vpn

R1#ping 3.3.3.3 source lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
.....
Success rate is 0 percent (0/5)

ASA3(config)# logging on
ASA3(config)# logging console 7

%ASA-3-106014: Deny inbound icmpsrc outside:1.1.1.1(LOCAL\10.0.0.1) dst
inside:3.3.3.3 (type 8, code 0)
```

So we have to either explicitly allow this traffic on outside interface OR just enable back this command.

```
ASA3(config)# sh run access-list
access-list OUTSIDE_IN extended permit icmp any any
ASA3(config)# sh run access-g
ASA3(config)# sh run access-group
```

```
access-group OUTSIDE_IN in interface outside
```

****allowing by access-list we have to allow all the required traffic*****

```
R1#ping 3.3.3.3 source lo0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/91/116 ms
```

OR

```
ASA3(config)#  sysopt connection permit-vpn

****this will automatically allow all the traffic on tunnel interface as ASA consider
IPsec tunnel interface as security level 100*********
```

UniNets Document