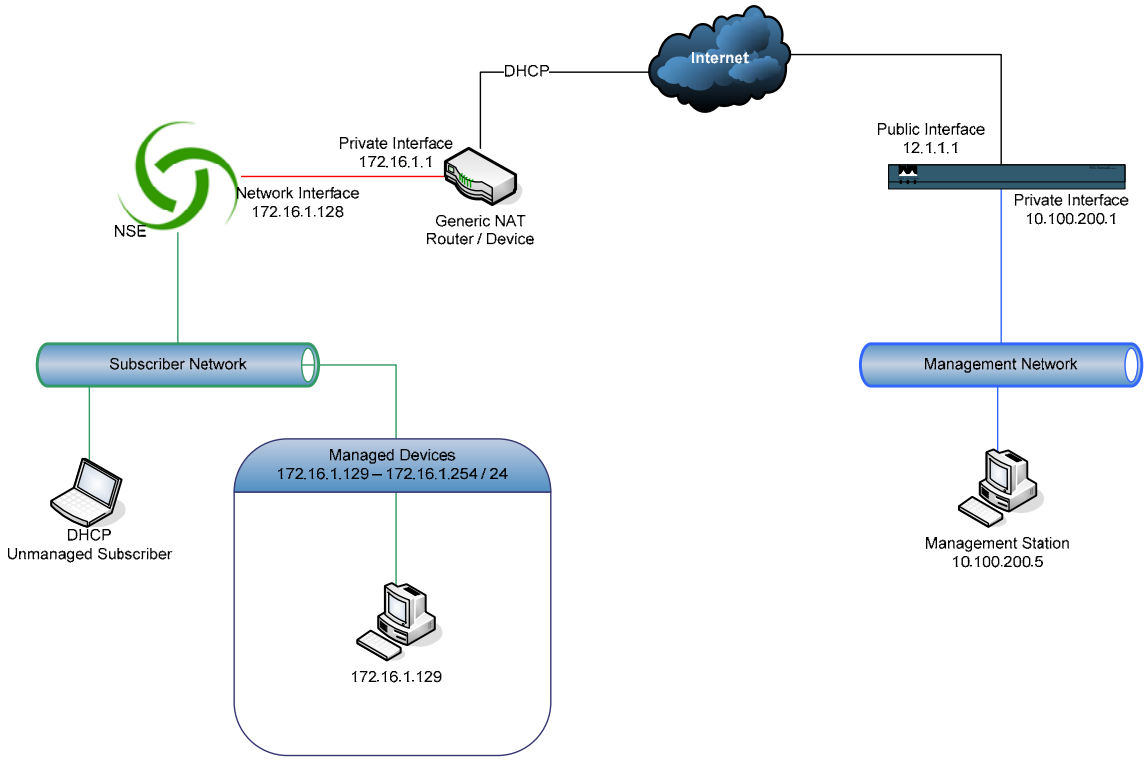
Configuration Summary

This document describes configuring an NSE initiated IPSec tunnel from behind a NAT device to a VPN endpoint for the purpose of managing devices inside the NSE subscriber interface from a NOC environment.

In this example, the following configuration is assumed:



1. **NAT Device**
   - Provided by ISP; configuration is static and cannot be modified
   - Obtains external (public) address via DHCP
   - Internal interface address is **172.16.1.1 / 24**
   - Internal DHCP server configured with an address pool of **172.16.1.2 - 172.16.1.127**
   - Device supports IPSec pass-thru (and is enabled)

2. **NSE**
   - Network interface statically configured as **172.16.1.128** (outside internal DHCP pool on NAT device)
   - Devices to be managed are addressed in the **172.16.1.129 - 172.16.1.254** network range.

3. **VPN Terminator (NOC)**
   - A Cisco PIX appliance is installed and configured at the NOC
   - External (public) address is 12.1.1.1
   - Internal network is 10.100.200.0 / 24

Configuring the VPN Terminator

1. We must first create the access control lists that will be used in the configuration.

   The first will be applied to prevent NAT on our outbound IPSec traffic --

   ```
   access-list nonat permit ip 10.100.200.0 255.255.255.0 172.16.1.0
   255.255.255.0
   ```

   Next, we will specify the ACL that will be used in our dynamic crypto map –

   ```
   access-list managed_networks permit ip 10.100.200.0 255.255.255.0
   172.16.1.0 255.255.255.0
   ```

2. Bind the "**nonat**" ACL created above to the inside interface. This command instructs the PIX not to perform NAT on packets that match our ACL; which in this case is the traffic between our management network and the remote subscriber network --

   ```
   nat (inside) 0 access-list nonat
   ```

3. The PIX must be configured to explicitly allow IPSec connections –

   ```
   sysopt connection permit-ipsec
   ```

4. Now, we'll configure the IPSec parameters (transform-set), setup our dynamic map using the ACL we created in step 1.

   In this example, we'll be using **ESP** with **3DES** encryption and **MD5** authentication. The dynamic map for our managed networks will be configured with sequence **10**, and we'll call it "**managed_networks_dynmap**" –

   ```
   crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
   crypto dynamic-map managed_networks_dynmap 10 match address
   managed_networks
   crypto dynamic-map managed_networks_dynmap 10 set transform-set ESP-
   3DES-MD5
   ```

   Now that we've created our dynamic map, we need to associate it with the crypto map

and outside interface of the PIX. We'll also specify that we want to use **ISAKMP** with this map entry. We'll call the crypto map entry "**dyn-map**" and once again use sequence **10** --

```
crypto map dyn-map 10 ipsec-isakmp dynamic managed_networks_dynmap
crypto map dyn-map interface outside
```

5. Finally, we need to setup the ISAKMP policy that will be used to accept connections.

   In this example, we'll be using a pre-shared key set to "**nomadix**". Note that the key entry specifies "**0.0.0.0**" for address and netmask; this allows the key to be used with multiple (dynamic) endpoints.

   As with ESP, we'll use **3DES** encryption and **MD5** authentication in this ISAKMP policy. In addition, we're specifying DH Group 2 (1024 bit) strength, and a key lifetime of **86400** seconds.

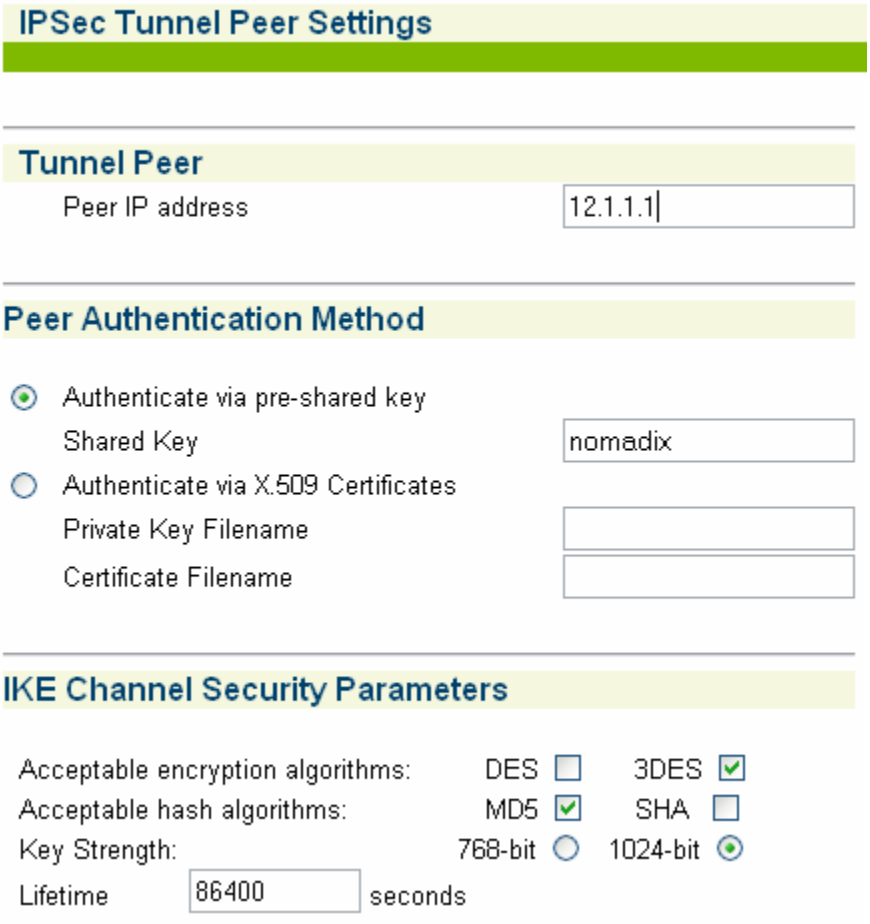
   Notice the policy sequence number; be sure this number matches your **crypto map** entry from the previous step (**10** in this example) --

```
isakmp enable outside
isakmp key nomadix address 0.0.0.0 netmask 0.0.0.0
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
```

Configuring the NSE

Before continuing, make sure that IPSec is enabled on your NSE. You can find the setting in Configuration->IPSEC. Enabling will require a reboot of the NSE before you will be able to continue with the configuration.

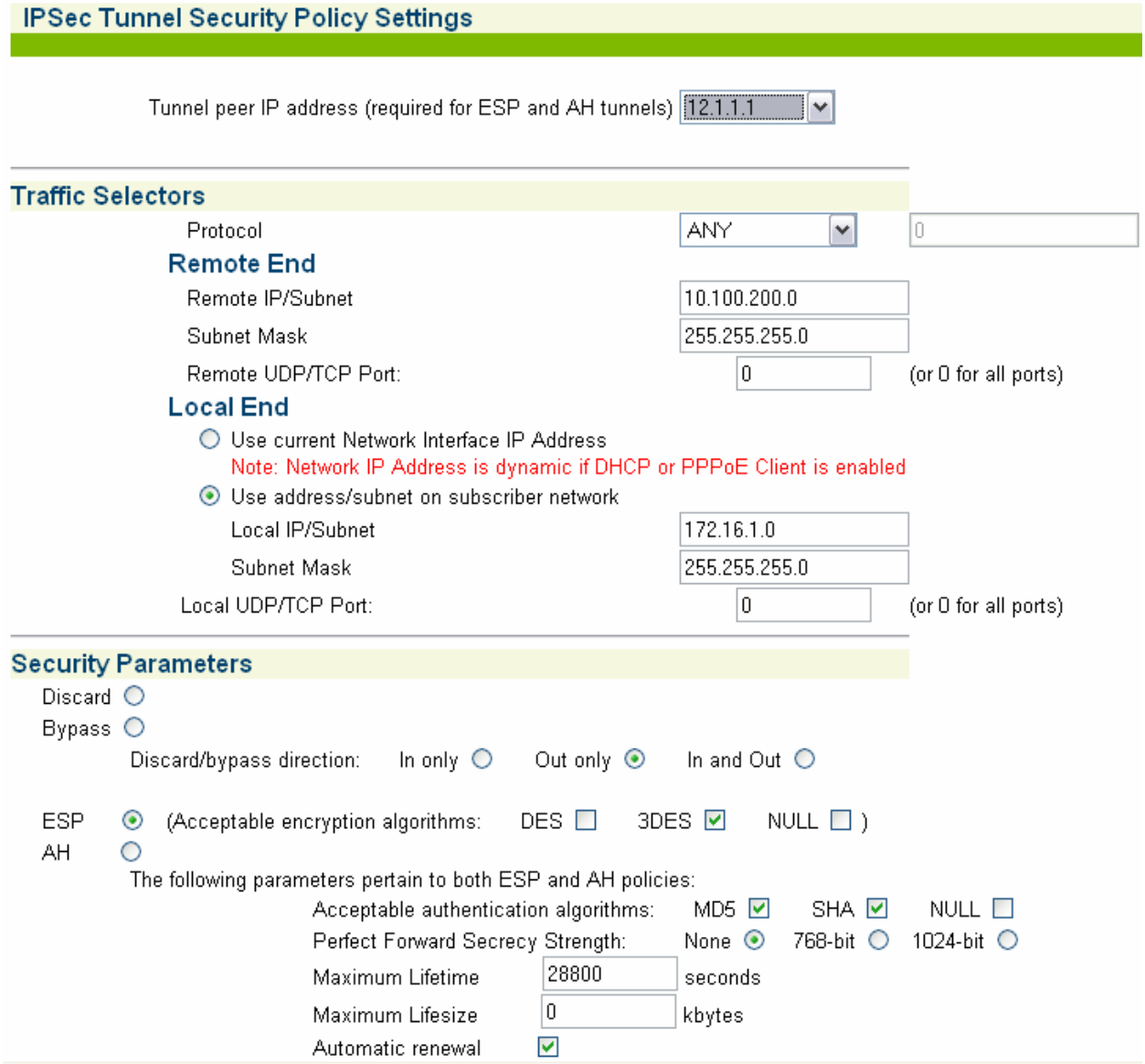
1. The first step is to configure our IPSec peer – in this example, the PIX firewall we configured in the prior section. Note that the **IKE Channel Security Parameters** must match the **ISAKMP** policy as configured on the peer; **3DES, MD5, Group2 (1024-bit)**



2. Next, we'll setup the IPSec policy that specifies the traffic to send to a given endpoint. Be sure you select the peer you configured in the previous step.

   Configure the remote and local addresses (in this example, we will specify a local address rather than using the network interface address)

   Configure the security parameters to match the IPSec parameters we setup in the prior section. (ESP-3DES-MD5, no perfect forward secrecy)



3. Finally, we need to specify the devices that will be managed and configure them as permanent entries in the subscriber table.

   Note that we are adding this subscriber profile as a **Device.**