



# FortiNAC

## Cisco VPN ASA Device Integration

Version: 9.1

Date: June 15, 2023

Rev: T

**FORTINET DOCUMENT LIBRARY**

<http://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<http://video.fortinet.com>

**FORTINET KNOWLEDGE BASE**

<https://community.fortinet.com/t5/Knowledge-Base/ct-p/knowledgebase>

**FORTINET BLOG**

<http://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<http://support.fortinet.com>

**FORTINET COOKBOOK**

<http://cookbook.fortinet.com>

**NSE INSTITUTE**

<http://training.fortinet.com>

**FORTIGUARD CENTER**

<http://fortiguard.com>

**FORTICAST**

<http://forticast.fortinet.com>

**END USER LICENSE AGREEMENT**

<http://www.fortinet.com/doc/legal/EULA.pdf>



# Contents

- Overview ..... 5
  - About this Document..... 5
  - What It Does..... 5
  - Requirements ..... 6
  - Considerations..... 7
- Integration ..... 8
  - Configure ASA..... 8
    - IP Pool ..... 8
    - Open (Unrestricted) Network Object Group ..... 8
    - Restricted Network Object Group ..... 8
    - ACL ..... 9
    - Tunnel Group Policy ..... 11
    - Tunnel Group..... 12
    - Syslog ..... 13
  - Configure FortiNAC ..... 14
    - Isolation Interfaces ..... 14
    - Policy Based Routes..... 16
    - Authentication Server Settings ..... 18
    - Model ASA in Inventory ..... 18
    - Develop Default Endpoint Compliance Policy ..... 20
    - Network Access Policies..... 22
    - Captive Portal ..... 24
    - Persistent Agent Configuration..... 25
    - Disable Captive Network Assistant ..... 26
- Validate ..... 28
- Troubleshooting ..... 30
  - Communication Using Virtual IP (VIP) in L2 High Availability Configurations ..... 30
  - Related KB Articles..... 31
  - Debugging..... 31
- Appendix ..... 32
  - How It Works..... 32
  - DNS File Entry Descriptions ..... 35
  - Policy Based Routing..... 37

Disable Persistent Agent Notifications.....	40
Address VPN Connection Delays .....	41
ASA CLI Commands Used by FortiNAC .....	42
Modifying IP List in Restricted Network Object Group .....	42
Disable Windows Browser Popups.....	42

# Overview

## About this Document

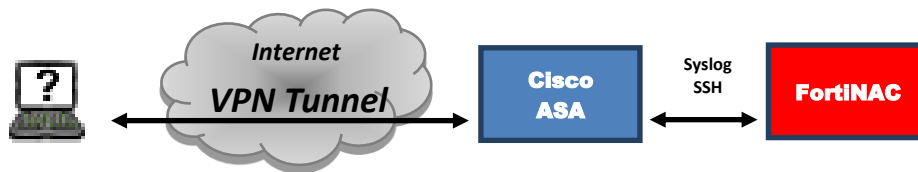
The information in this document provides guidance for configuring the Cisco ASA VPN device to be managed by FortiNAC. This document details the items that must be configured.


**Note:** As much information as possible about the integration of this device with FortiNAC is provided. However, the hardware vendor may have made modifications to the device's firmware that invalidate portions of this document. If having problems configuring the device, contact the vendor for additional support.

**Tip:** For hyperlinks referencing other documentation, right-click the link and select **Open in New Tab**.


## What It Does


FortiNAC controls access to the remote user's device connecting over the VPN. In order for the device to be able to gain access the network, FortiNAC must know about the connecting device and verify the device is in good standing.



1. When a device initially connects over a VPN tunnel, the device is restricted. 

2. FortiNAC identifies the device as known and trusted. 

3. The device is unrestricted. 

4. If configured for endpoint compliance, the device's security posture is evaluated. Network access is restricted upon failure. 

For more details on this process, see [How it Works](#) in the Appendix.

# Requirements

## FortiNAC

- Supported Engine Version: 8.3 or greater
- Recommended Engine Version: 8.6.4, 8.7.2 or greater (supports policy-based routing. See [Appendix](#).)
- Remote device must have either the FortiNAC Dissolvable or Persistent Agent
  - Supported FortiNAC Agent Version: 5.2 or greater
  - Agent Supported Operating Systems:
    - Windows (not Windows CE)
    - MAC OS
    - Linux
    - Android

Note: FortiNAC doesn't have an app or agent for iOS. Therefore, iOS mobile devices cannot connect through VPN.

- Dissolvable Agent can be downloaded as part of the VPN connection process from the Captive Portal
- Persistent Agent can also be downloaded from the Captive Portal or pre-installed
- Operating systems that cannot run a FortiNAC agent will always remain isolated when connecting to a VPN that is managed by FortiNAC
- Remote device firewall settings must allow TCP 4568 (bi-directional) for agent communication with FortiNAC

## ASA

- Cisco Adaptive Security Appliance firmware (ASDM and Firepower Threat Defense firmware *not* supported)
- SNMP community or account (v1/2/3 with read privilege)
- Account for SSH access (read/write privilege).
  - FortiNAC login sequence requires username, password and enable password.
  - If multiple accounts are used (due to multiple ASA's), all accounts must use the same level of access
  - SSH Allowed Access List should include the FortiNAC eth0 subnet. Based on customer experience, it is not recommended to use an open Allowed Access List (0.0.0.0) for SSH access on the ASA. See KB article [197942](#).
- **Build and Validate Test Configuration:** Before integrating a device with FortiNAC, set the device up to ensure that it is working correctly.
  - Create new VPN environment identical to production environment.
  - Confirm that hosts can connect to the device and access the network.
- If multiple ASAs are modeled/managed by FortiNAC, each ASA's restricted group must have unique individual IP addresses. They should not overlap.

## Considerations

- Cisco ASA Cluster Mode is not supported at this time.
- IPv6 is not supported.
- When configuring Restricted Object Groups in the Cisco ASA for VPN Integration, individual IP address entries must be added to the object group as opposed to a range. For details see [Restricted Network Object Group](#).
- **Automated Captive Portal Detection:** Devices that sense captive networks may trigger browsers during initial connection. To avoid this, automated captive portal detection must be disabled for VPN connections in FortiNAC. Instructions provided in section **Disable Captive Network Assistant**.
- **Split Tunnels:** Whether or not split tunnel (certain traffic doesn't go over tunnel) or full tunnel (all traffic goes over tunnel) is configured is dependent upon the customer requirements.
  - If the Dissolvable Agent (DA) will be used, it is recommended to disable split-tunneling for the VPN configured on the FortiGate. This ensures user's browser is automatically redirected to the URL where they can download the run-once agent.
  - FortiNAC validates endstation after the tunnel is established. In order to do that, initial access is restricted. Once confirmed, restricted access is lifted. In full tunnel implementations, there will be interruption on applications that are running prior to connecting.
- **Windows machines:** Recommended to disable browser popups on managed machines. See [Disable Windows Browser Popups](#) in the Appendix.
- Remote clients connecting to the network through a FortiNAC-managed VPN cannot be connected to a local network that is also being managed by FortiNAC within the same management domain.
- **Layer 3 High Availability:** Due to a limitation in the ASA, after a FortiNAC appliance failover, the following will not work without manual intervention:
  - VPN clients will be unable to access the captive portal pages
  - VPN clients with the persistent agent will not be on-boarded

For details, see [Tunnel Group Policy](#).

- This solution does not work in an environment using Cisco Dynamic Access Policies (DAP).
- If using Cisco AnyConnect VPN software and a macOS client with FortiNAC, make sure that the Web Security and Posture settings are both disabled. Otherwise, the AnyConnect software will not work with FortiNAC.

# Integration

## Configure ASA

### IP Pool

Configure the ASA to provide DHCP to the VPN clients by creating an IP Pool.

**External DHCP Servers:** If using an external DHCP server to provide addresses to the VPN clients, do not configure an IP Pool. Instead, configure the ASA to forward the DHCP requests to the DHCP server, then proceed to section [Restricted Network Object Group](#).

1. Configure an IP Pool that contains the addresses available for the ASA to assign for VPN connections managed by FortiNAC. This scope will also be defined in FortiNAC as the **VPN DHCP scope** in a later section.

**Command:**

```
ip local pool <IP POOL NAME> <IP scope of VPN clients> mask <DOTTED  
DECIMAL MASK>
```

2. Set the IP Pool reuse delay time. This prevents the next user who logs in to get the previous user's IP.

**Command:**

```
vpn-addr-assign local reuse-delay 5
```

### Open (Unrestricted) Network Object Group

Create an Object Group called **NSOpenGroup**. This group is used by FortiNAC to contain addresses that are no longer restricted.

**Command:**

```
object-group network NSOpenGroup
```

### Restricted Network Object Group

Create an object group for restricted access (restricted network object group). This is required for both visibility and control purposes.

**Important:** If multiple ASAs are modeled/managed by FortiNAC, each ASA's restricted group must have unique individual IP addresses. They should not overlap.

1. Run the command:

```
object-group network <RESTRICTED OBJECT GROUP NAME>
```



2. Add a network object entry for *each* IP address available for the ASA to assign FortiNAC managed VPN connections. FortiNAC reads this object group to identify the list of managed VPN IP addresses.
  - Must be in dot notation (not an alias).
  - Entries must match those of IP Pool (if created).
  - **Important:** Individual IP address entries must be added to the object group as opposed to a range.

**Commands:**

```
network-object host <IP address of HOST>
network-object host <IP address of HOST>
network-object host <IP address of HOST>
```

**Example:**

```
network-object host 10.19.58.5
network-object host 10.19.58.6
network-object host 10.19.58.7
network-object host 10.19.58.8
```

**Note:** If the IP address list is modified at a later date, the restricted Object group must be re-read. See [Modifying IP List in Restricted Network Object Group](#) in the Appendix.

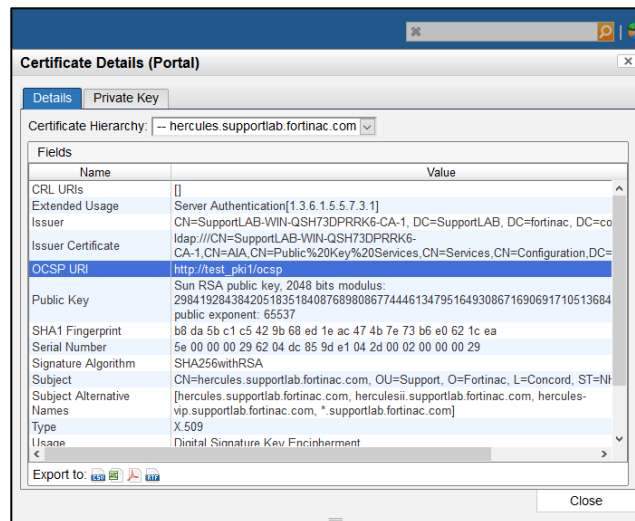
## ACL

### Identify the OCSP URI for SSL Certificate Authentication

For successful interaction with the Captive Portal or Persistent Agent within the restricted network object group, hosts must be able to validate SSL certificates. In order for validation to complete, access from the restricted object group to the IP address of the certificate's **OCSP URI** must be allowed.

**Note:** If using 3<sup>rd</sup> party public certificates and internet traffic does not cross the VPN tunnel (split tunnel configurations) this is not necessary. Skip this step and proceed to [ACL Configuration](#).

1. In the FortiNAC Administration UI, navigate to **Security Configuration > Certificate Management**.
2. Select the **Portal** target and click **Details**.
3. If using the Persistent Agent, select the **Persistent Agent** target and click **Details**.



## ACL Configuration

Configure the ACL to be applied as the VPN filter by the Tunnel Group Policy. This ACL is specifically developed to ensure control of VPN clients prior to agent communication.

L3 High Availability environments (Primary and Secondary servers reside on different subnets): ACL rules must also account for communication to the Secondary Server VPN Isolation interface. Otherwise, VPN traffic will not be forwarded to the Secondary server VPN interface upon failover.

### Commands:

```
##Allow any IP in the Object group to communicate with Primary FortiNAC
VPN IP address##
```

```
access-list <ACCESS LIST NAME> extended permit ip object-group
<RESTRICTED OBJECT GROUP NAME> host <IP address of Primary FortiNAC VPN
isolation interface>
```

```
##(L3 High Availability configurations only) Allow any IP in the Object
group to communicate with Secondary FortiNAC VPN IP address##
```

```
access-list <ACCESS LIST NAME> extended permit ip object-group
<RESTRICTED OBJECT GROUP NAME> host <IP address of Secondary FortiNAC VPN
isolation interface>
```

```
##Allow any IP in the Object group to communicate with the OCSP URI for
certificate authentication##
```

```
access-list <ACCESS LIST NAME> extended permit ip object-group
<RESTRICTED OBJECT GROUP NAME> host <IP address of OCSP URI>
```

```
##Block any IP in the Object group from communicating to any other
destination##
```

```
access-list <ACCESS LIST NAME> extended deny ip object-group <RESTRICTED  
OBJECT GROUP NAME> any
```

```
##Block any DNS traffic to Primary FortiNAC VPN IP address##
```

```
access-list <ACCESS LIST NAME> extended deny udp any host <IP address of  
Primary FortiNAC VPN isolation interface> eq domain
```

```
##(L3 High Availability configurations only) Block any DNS traffic to  
Secondary FortiNAC VPN IP address##
```

```
access-list <ACCESS LIST NAME> extended deny udp any host <IP address of  
Secondary FortiNAC VPN isolation interface> eq domain
```

The ACL line below will allow full access. You may choose to modify this line to further restrict access if needed. (i.e.- Allow only RDP access to a given subnet)

**Command:**

```
access-list <ACCESS LIST NAME> extended permit ip any any
```

## Tunnel Group Policy

Each Tunnel Group must have a default Tunnel Group Policy that is assigned to connecting user device. This policy controls network access and must have the following:

- VPN filter (to apply ACL restricting access)
- IP Pool (configured above) for VPN access managed by FortiNAC (not needed if using external DHCP server for VPN)
- DNS

A connected user device is assigned a production IP address and DNS server(s) by ASA.

Example:

FortiNAC CA Server name: Server01.Fortinet.com

Eth0: 10.10.200.147

Registration: 10.10.201.130

Remediation: 10.10.201.131

VPN: 10.10.201.132

VPN DHCP Scope (IP Pool): 10.19.58.0/23

Eth1 GW: 10.10.201.129

VPN user's ipconfig output (existing configuration)

DHCP Server . . . . . : 10.12.14.1

DNS Servers . . . . . : 192.168.7.11, 192.168.7.12

The following modifications are required to support automatic DNS redirection:

1. For non-restricted access, DNS servers (7.11 and 7.12) must resolve the FortiNAC Server name to the **eth0 IP address**.

Example: Server01.Fortinet.com -> 10.10.200.147

2. DNS server list provided by DHCP needs to include the **eth1 VPN sub-interface IP address** as the secondary DNS server:

Example: VPN user's ipconfig output (where VPN IP address = 10.10.201.132):

DNS Servers . . . . . : 192.168.7.11, **10.10.201.132**

**L3 High Availability Consideration:** As of this writing, the ASA only supports two entries for DNS. Consequently, VPN clients are unable to access the captive portal pages after an appliance failover. The workaround is to update the DNS server entry in the ASA from the Primary Server VPN interface IP address to the Secondary Server VPN interface. This change must be reverted after control is resumed to the Primary Server. See related [KB article 190423](#). For more information on the DNS configuration, refer to Cisco ASA documentation.

**Split Tunneling:** If split tunneling is configured, the user is not automatically redirected to the agent download page. Inform users of the specific web page to browse to for the agent download.

3. Default domain value must match the domain name to be configured in Configuration Wizard. NOTE: If FNAC is managing multiple VPN scopes, they must all use the same domain.

### Commands:

VPN users admitted under the specified policy are to be controlled by the ACL <ACCESS LIST NAME> and assigned IPs from <IP POOL NAME>.

```
group-policy <GROUP POLICY NAME> internal
group-policy <GROUP POLICY NAME> attributes
//dns-server values are specifically ordered.
dns-server value <IP address of production DNS server> <IP
address of FortiNAC VPN isolation interface>
vpn-filter value <ACCESS LIST NAME>
default-domain value <REAL DOMAIN NAME>  << Also used in FortiNAC scope
address-pools value <IP POOL NAME>
```

## Tunnel Group

Configure a Tunnel Group for users that will be authenticated and scanned by FortiNAC.

**Connecting using IPsec:** This tunnel group is the one configured in the connection profile installed on each user's PC.

Each Tunnel Group has a default Tunnel Group Policy that controls network access. FortiNAC supports IPsec and SSL tunnel types. The default Tunnel Group Policy is used to contain those addresses that are restricted according to the Tunnel Group Policy.

**Important:** To allow registered hosts to connect to the network through tunnel groups that are not managed by FortiNAC, make sure those unmanaged tunnel groups are configured on the VPN device such that IP traffic back to the management and portal IPs of FortiNAC is not permitted. This prevents the Persistent Agent on the remote machines from contacting the FortiNAC server with the results of the host scan. If the Persistent Agent contacts FortiNAC, the user may see unexpected pop-ups from the agent.

#### Commands:

```
tunnel-group <TUNNEL GROUP NAME> type remote-access
tunnel-group <TUNNEL GROUP NAME> general-attributes
address-pool <IP POOL NAME> << Not needed if IP Pool was not configured
default-group-policy <GROUP POLICY NAME>
```

## Syslog

Using either the CLI or the user interface for the Cisco ASA, configure the following settings:

- Verify logging is enabled.
- Create an event list with the following:
  - Name
  - Range of syslog message IDs **737006-737026** and **722051**  
**Note:** FortiNAC processes all inbound messages. For best performance, it is recommended to limit the IDs sent to ones listed.
- Configure the logging filter for Syslog Servers by selecting the event list in the previous step.
- Add the FortiNAC Server or Control Server as a Syslog server. The Interface name should be set appropriately and the IP address should be the eth0 or management IP address of the FortiNAC Server or Control server. If FortiNAC is configured for High Availability, add the Secondary Server eth0 IP address as well.
- In the Syslog Setup, verify the messages in the ID range configured are enabled.
- Interface name = Interface with the IP address to be used for communication with FortiNAC.

#### Commands:

```
logging enable
logging list <list name> message 737006-737026
logging list <list name> message 722051
logging trap <list name>
logging host <interface name> <FortiNAC eth0 IP address>
logging host inside <interface name> <Secondary FortiNAC eth0 IP address> <<
Add if High Availability is enabled
```

## Configure FortiNAC

The following items must be configured on the FortiNAC (FNAC) appliance:

- VPN Isolation interface (including DHCP scopes and domain name)
- Policy Based Routes
- RADIUS/LDAP Authentication
- ASA model creation/discovery
- ASA model configuration
- VPN Endpoint compliance policies
- VPN Network Access Configuration policies
- VPN Captive Portal Content

### Isolation Interfaces

Configure the eth1 VPN isolation interface using Configuration Wizard. Refer to the [Configuration Wizard](#) reference manual in the Fortinet Document Library for instructions.

**High Availability:** If High Availability is configured, access Configuration Wizard on the Secondary Server and make the same modifications. This ensures the domain value and the additional scopes are added properly in the event of a failover.

### Virtual Private Network Field Definitions

#### Virtual Private Network Interface eth1

<b>Interface IPv4 Address</b>	IPv4 address for the VPN interface on eth1.
<b>Mask</b>	VPN interface subnet mask (IPv4).
<b>IPv4 Gateway</b>	Gateway IP address used by the VPN interface
<b>Interface IPv6 Address (currently not supported)</b>	IPv6 address for the VPN interface on eth1.
<b>Interface IPv6 Mask in CIDR notation (currently not supported)</b>	Subnet IPv6 mask for the VLAN interface in CIDR notation format (e.g., 64).
<b>Interface IPv6 Gateway (currently not supported)</b>	IPv6 Gateway for the VLAN interface for eth1 when clients connect through this VLAN.

**3<sup>rd</sup> Party DHCP Server for Restricted Clients:** If using a DHCP server other than FortiNAC for restricted VPN clients, do the following:

1. Create a lease pool with a dummy range.
2. Add VPN IP subnet to VPN IP Subnets field at the bottom of the page. This will allow FortiNAC to answer DNS requests.

### Virtual Private Network Scopes

Label	Desired name for VPN DHCP scope
<b>Lease Pool Start</b>	<p>Starting IP address that delineates the range of IP addresses available to be managed by FortiNAC over the VPN tunnel.</p> <p>The VPN DHCP scope(s) must match the IP Pool (if configured) and the Restricted Network Object Group on the ASA. Although FortiNAC does not provide DHCP addressing for the VPN clients, certain files are updated with this information to allow proper handling of DNS SRV queries from agents and captive portal page display.</p>
<b>Lease Pool End</b>	<p>Ending IP address that delineates the range of IP addresses available to be managed by FortiNAC over the VPN tunnel.</p> <p>The VPN DHCP scope(s) must match the IP Pool (if configured) and the Restricted Network Object Group on the ASA.</p>
<b>Domain</b>	<p>Must match the domain value configured in the ASA.</p> <p><b>NOTE:</b></p> <ul style="list-style-type: none"> <li>• FortiNAC only answers SRV queries from connecting agents sourced from this domain. If FortiNAC is managing multiple VPN scopes, they must all use the same domain. See <a href="#">DNS File Entry Descriptions</a> in the Appendix for details.</li> <li>• OS X, iOS, and some Linux systems may have communication issues if a .local suffix is used.</li> </ul>
<b>Lease Time</b>	<p>Time in seconds that an IP address in this domain is available for use. When this time has elapsed the user is served a new IP address. The recommended lease time is 60 seconds.</p>

#### Example:

FortiNAC CA FQDN: Server01.Fortinet.com

Eth0 (Management interface): 10.10.200.147

Registration: 10.10.201.130

Remediation: 10.10.201.131

VPN: 10.10.201.132

VPN DHCP Scope (IP Pool): 10.19.58.0/255.255.254.0

Eth1 GW: 10.10.201.129

After committing the changes in Configuration Wizard, run `ifconfig` in the CLI to identify the sub-interfaces assigned to the isolation networks. If separate Control and Application Servers, access the CLI of the Application Server.

```
> ifconfig
```

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 10.10.200.147 netmask 255.255.255.0 broadcast 10.10.200.255

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 10.10.201.130 netmask 255.255.255.0 broadcast 10.10.201.255

eth1:1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 10.10.201.131 netmask 255.255.255.0 broadcast 10.10.201.255

eth1:2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 10.10.201.132 netmask 255.255.255.0 broadcast 10.10.201.255
```

## Policy Based Routes

Configure policy-based routing. Policy-based routing ensures traffic is transmitted out the same interface on which it was received. It is needed primarily on Control/Application servers that contain both the primary and isolation interfaces on which the agent can communicate.

Policy-based routing is configured on FNAC using the command: ***setupAdvancedRoute*** which is run from a FNAC CLI. This must be done for both Primary and Secondary Servers in High Availability Configurations. For details on policy based routing and the script used for configuration, see [Policy Based Routing](#) in the Appendix.

If High Availability configuration, perform the following steps on the Secondary server also.

1. Have available the gateway information for all FortiNAC interfaces (eth0, eth1, etc).
2. Login to the CLI as root of the FortiNAC server (Application Server if separate Control and Application Servers)



3. Run the script

**Important:** The following instructions presume the script has not yet been run. If script has been run previously and are modifying or adding an interface, see [Appendix](#) for instructions.

- a. Type **setupAdvancedRoute**
- b. Type **I** to install
- c. Enter the gateway for each interface (eth0, eth1, etc) as prompted.

4. Once script completes, verify configuration. Type

**ip rule show**

There should now be a rule listed for each interface and sub-interface configured:

```
0: from all lookup local
10: from <eth0 IP address> lookup eth0
20: from <eth1 IP address> lookup eth1
30: from <eth1:1 IP address> lookup eth1:1
40: from <eth1:2 IP address> lookup eth1:2
50: from <eth1:3 IP address> lookup eth1:3
32766: from all main
32767: from all default
```

Example:

```
>ip rule show
0: from all lookup local
10: from 10.10.200.147 lookup eth0
20: from 10.10.201.130 lookup eth1
30: from 10.10.201.131 lookup eth1:1
40: from 10.10.201.132 lookup eth1:2
32766: from all main
32767: from all default
```

5. Reboot appliance. Type

**shutdownNAC**

*<wait 30 seconds>*

**shutdownNAC -kill  
reboot**

## Authentication Server Settings

Before network access is permitted, rogue hosts connecting to the VPN must register with FortiNAC via the captive portal or Persistent Agent. If it is not desired to register unknown hosts connecting to the VPN, skip this step.

Configure FortiNAC to authenticate using either a RADIUS server or LDAP directory. Refer to the Administration Guide sections listed below for instructions. Depending upon the deployment, these components may already be configured.

- Define which authentication server type will be used (LDAP or RADIUS). See [Portal configuration – Configure authentication credentials](#)
- Configure the settings for the authentication server. Refer to the appropriate section: [Configure RADIUS settings](#)
- [Directory configuration](#)

## Model ASA in Inventory

### Select Cisco ACS Account for Access to ASA

FortiNAC requires access to the VPN device. When the VPN device is modeled in FortiNAC, a user name and password are required to set up this communication. The account associated with that user name and password must exist on the Cisco ASA's authentication server.

FortiNAC can use credentials for an admin account with full rights to the Cisco ASA or for a TACACS account that has limited access. If choosing to use an account with limited access, ensure the commands [listed in the Appendix](#) are accessible and executable.

### Add Device Model

Create or discover the FGT in FNAC, if it does not already exist, to manage its VPN users connecting to the network via a VPN connection. In order to integrate FNAC and the FGT, they must be able to communicate using multiple protocols, including SSH, SNMP and FSSO. Each of these have their own requirements.

1. In the FortiNAC Administration UI, navigate to **Network > Inventory**.
2. Model the ASA. Instructions in the Administration Guide:

Single device: [Add or modify a device](#)

Multiple devices: [Discovery](#)

**Note:** If a “?” appears as the icon, then support needs to be added for that device. See KB article [Options for Devices Unable to Be Modeled in Topology](#) for instructions.

### **Modeling ASA's with a Virtual IP (VIP):**

- Model using the VIP only.

- The SSH key used by FortiNAC to communicate with the ASA could change based upon which ASA owns the VIP. To ensure the proper SSH keys are used when communicating with the ASA, log in to the FortiNAC CLI as root and run the command:

```
device -ip <VIP> -setAttr -name MultiKnownHostEntries -value true
```

3. Select the new device and click **Model Configuration**. Refer to [Model Configuration](#) section of the **Administration Guide** in the Fortinet Document Library for additional information.
4. Enter the information required in the configuration window, then click **Apply**.

### VPN Device Model Configuration Field Definitions

Field	Definition
<b>General</b>	
<b>User Name</b>	The user id required for communication with the device.
<b>Password</b>	The password required to connect to the device.
<b>Enable Password</b>	The enable password for this device (required).
<b>Read Groups</b>	Connect to the device and read the group policy information into the FortiNAC database.
<b>Protocol</b>	
<b>Type</b>	Protocol used for connection to the device. Options are Telnet, SSH1, or SSH2
<b>Restricted Access</b>	
<b>Object Group Name</b>	Name of the <a href="#">Restricted Network Object Group</a> configured in the ASA (case sensitive). <b>Important:</b> Name must exactly match.

## Develop Default Endpoint Compliance Policy

Create a default VPN policy to:

- Prompt to download an agent for isolated machines that do not have an agent already installed.
- Scan the machine to determine security posture based on matching the user/host profile in the VPN Endpoint Compliance Policy.

### Create Security Scan

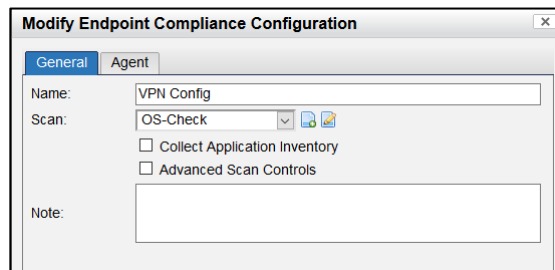
1. Navigate to **Policy & Objects > Policy Configuration**.
2. Under **Endpoint Compliance** click **Scans**.
3. Configure the scan to check for required programs and/or files. For more details, refer to the following section in the Administration Guide: [Add or modify a scan](#)

**Note:** Since a device remains in an isolated state until the scan completes, the complexity of the scan may introduce delays in the time it takes the remote user to complete the connection process.

### Create Endpoint Compliance Configuration

Create an Endpoint Compliance Configuration to assign an agent and the security scan.

1. Under the **General** tab, select the scan created for the VPN connection.
2. For better performance, it is recommended to de-select **Collect Application Inventory**.



3. Click the **Agent** tab.
4. Select the agent type and version to provide to connecting computers that do not have an agent installed. There are three agent types:
  - **Persistent Agent (PA):** Installed on the user's PC and remains there, communicating with FortiNAC whenever the PC is on the network.

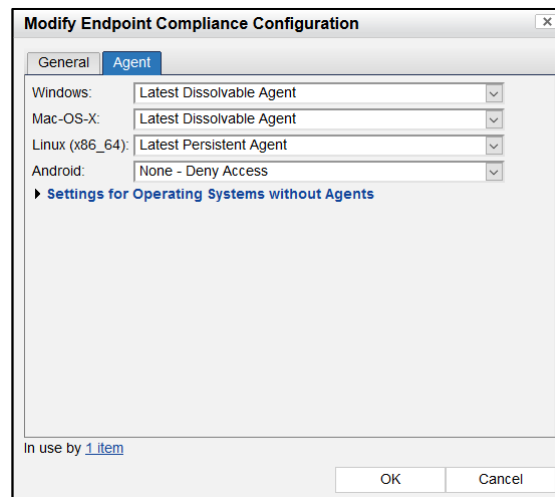
**Note:** It is recommended to enable the **Restrict Roaming** Persistent Agent setting when connecting over VPN managed by FortiNAC. For details on this setting, refer to section **Persistent Agent Settings** of the [Persistent Agent Configuration and Deployment](#) reference manual in the Fortinet Document Library.

- **Dissolvable Agent (DA):** Downloaded and installed every time the user connects to the network. After scanning the user's PC and reporting results to FortiNAC, the agent removes itself.

**Note:**

- It is recommended users are sent to the download location through DNS and URL redirection.
  - It is recommended to disable split-tunneling for the VPN configured on the FortiGate. This ensures user's browser is automatically redirected to the URL where they can download the run-once agent.
- **Mobile Agent:** Installed on a handheld device running Android and remains there, communicating with FortiNAC whenever the device is on the network.

**Note:** Due to unsupported features by the vendor, mobile devices running iOS cannot connect through VPN.



For more details, refer to the following section in the Administration Guide: [Add or modify a configuration.](#)

## **Create User/Host Profile**

Configure the User/Host Profile for the Endpoint Compliance policy.

1. Create a new User/Host profile. See below for criteria options.

### **Persistent Agent**

**Required:** Host [VPN Client: Yes]

**Optional:** Add other criteria as desired. Optionally with some other criteria to avoid undesired scanning of non-VPN offline hosts.

### **Dissolvable Agent**

**Required:** Adapter [Connected: Offline]

**Optional:**

Host [Persistent Agent: No]

Adapter [IP Address: <VPN IP subnets. Can use wildcard (\*)>]

2. Click **OK**.

**Note:** Hosts connecting to VPN via a local SSID will not match the “VPN Client: Yes” criteria.

For more details, refer to the following section in the Administration Guide: [User/host profiles](#).

## **Create Endpoint Compliance Policy**

Create the Endpoint Compliance policy using the User/Host Profile and Endpoint Compliance Configuration. Once created, adjust ranking as appropriate. For more details, refer to the following section in the Administration Guide: [Add or Modify a policy](#).

## **Network Access Policies**

Configure Network Access Policies if different levels of network access are required for different users with the same VPN connection profile.

By default, all users with the same VPN connection profile will have the same level of access. This is based on the Tunnel Group Policy that is associated with the connection profile's defined Tunnel Group. FortiNAC Network Access Policies can be used to provision different levels of network access by assigning the appropriate Tunnel Group Policy.

## **Configuration Steps**

### **ASA**

- Create multiple Tunnel Group Policies with the levels of network access required  
**Important:** The IP Pool must be the same as the IP Pool for the default Tunnel Group Policy

## FortiNAC

1. In the Administration UI, navigate to **Policy > Policy Configuration**
2. Create a **Device Group** and add the ASA device as a member
3. Create a separate **User/Host Profile** for each level of access (such as Staff and Executives):
  - Use the Device Group containing the ASA as the connection location
  - Make sure each user and associated host will match one of the User/Host Profiles
  - If using the DA, host connection status = Offline

### Example:

Host is connected over VPN (Location: Cisco ASA device group)

and

Registered or logged on user is a member of the “Users” LDAP group (Who What by Group: Users)

And

One or more of the following criteria apply:

Host has the Dissolvable agent (Host Connection Status: Offline)

Host has the Persistent Agent installed (Persistent Agent: Yes)

Host is detected as a VPN Client (VPN Client: Yes)

**Add User/Host Profile**

Name:

Where (Location):

Who/What by Group:

Who/What by Attribute:

When:

4. Create a separate **Network Access Configuration** for each VPN Tunnel Group Policy
5. Place the appropriate Tunnel Group Policy name in the Access Value/VLAN field  
**Important:** name spelling and case must match exactly
6. Create **Network Access Policies** to Map User/Host Profiles to Network Access Configurations
7. Adjust the rank of the Network Access Policy as appropriate

For more details, refer to the following section in the Administration Guide: [Network Access Policies](#)

## Captive Portal

### Develop Content

Configure the settings and behavior of the portal pages to be presented to users when connecting to the VPN. The following Content Fields are listed under the VPN branch in Content Editor (System > Portal Configuration)

Content	Description
<b>Index (Redirect)</b>	Presented to user while NAC evaluates host to determine which page to display.
<b>Download Page</b>	The VPN Login page displayed to hosts that connect with user information available from the VPN device, but do not have an agent.
<b>Profile Configuration Download</b>	If the host matches a supplicant (EasyConnect) policy, this page will allow them to download the Supplicant Configuration. This was primarily used for Apple iOS devices (not supported for VPN). Other devices that end up at this page will download the Agent.
<b>Mobile Agent Download</b>	A page presented to download the Agent from the relevant App store.
<b>Instructions</b>	Relates to the Download Page. Like other Login Forms, the optional instructions may be displayed inline in the download page or as a separate page opened from a link. "Instructions" option is selected in Download Page or User Login (In-line only) content.
<b>User Login (In-line only)</b>	Reached from VPN_Redirect when the user first hits the VPN context. If no user information can be found from the VPN device, then this login form is used.
<b>Success</b>	Host has successfully scanned and is released from isolation.

For more details, refer to the following section in the Administration Guide: [VPN Portal](#).

### Using Multiple Captive Portals with VPN

When Multiple Captive Portals are configured, Portal Policies are used to determine which portal is presented upon isolation. FortiNAC cannot properly determine the portal for VPN connections if the host does not have an Agent already installed. Therefore, the default portal should be used for VPN connections.

For more details, refer to the following section in the Administration Guide: [Portal Policies](#).



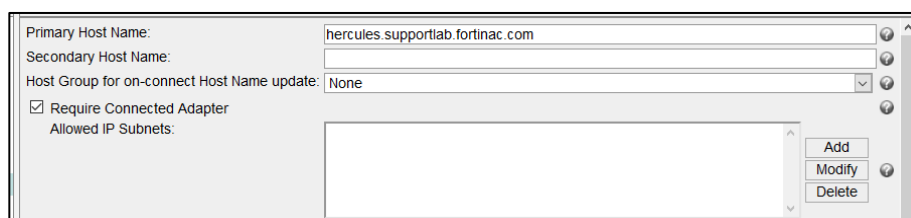
## Persistent Agent Configuration

### VPN Communication Using Required Connected Adapter

FortiNAC can be configured to only communicate with Persistent Agents connected to the local network. The option controlling this function is called **Require Connected Adapter**.

FortiNAC is unable to determine the online status for VPN connections. To allow FortiNAC to communicate with agents over VPN when this option is enabled, additional configuration is required.

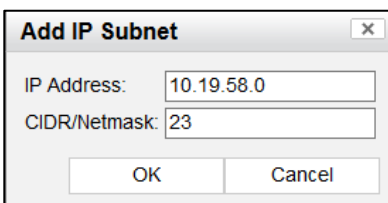
1. Navigate to **System > Settings > Persistent Agent > Security Management**.
2. Review the Require Connected Adapter setting.



The screenshot shows a configuration window with the following fields and controls:

- Primary Host Name: hercules.supportlab.fortinac.com
- Secondary Host Name: (empty)
- Host Group for on-connect Host Name update: None
- ☒ Require Connected Adapter
- Allowed IP Subnets: (empty list box)
- Buttons: Add, Modify, Delete

3. If **Require Connected Adapter** checkbox is selected, proceed to step 4. Otherwise, this section can be skipped.
4. Click the **Add** button next to **Allowed IP Subnets**.
5. Specify the network used for the VPN DHCP Scope then click **OK**. This allows FortiNAC to communicate with agents from that network regardless of connection status.



The 'Add IP Subnet' dialog box contains the following fields and controls:

- IP Address: 10.19.58.0
- CIDR/Netmask: 23
- Buttons: OK, Cancel

For more details, refer to the following section in the Administration Guide: [Security Management](#).

### Notification Messages

By default, the agent will display messaging to the user informing them of their network status when connecting over VPN.

When end stations first connect, access is restricted and the agent displays:  
**“Network restrictions have been applied for this device”**

Once FortiNAC has evaluated the end station and moved the IP address to the unrestricted network object group, the agent displays:  
**“Network restrictions have been lifted for this device”**

These messages will display regardless of the **ClientStateEnabled** Persistent Agent setting. For more information on this setting, see section **Persistent Agent Settings** in the Persistent Agent Deployment Guide: [Persistent Agent Deployment and Configuration](#)

It is possible to disable the messaging if desired. For instructions, see [Disable Persistent Agent Notifications](#) in the Appendix.

## Disable Captive Network Assistant

Devices that sense captive networks may trigger browsers because network connection is initially restricted.

### iOS/macOS/Samsung Android

FortiNAC must not have Captive Network Assistant configured. This feature is disabled by default. If enabled, see section **Disable CNA (iOS/macOS/Samsung Android)** in the [Captive Networks Assistant](#) reference manual.

**Note:** This function is disabled for all portals for these operating systems.

### Windows

By default, it is possible for Windows machines to automatically popup the default browser. Refer to the following article for more information:

<https://docs.microsoft.com/en-us/troubleshoot/windows-client/networking/internet-explorer-edge-open-connect-corporate-public-network>

The following options are available for disabling Windows Captive Portal Detection.

**Note:** These options are not necessary if only managed Windows machines are connecting and the Registry Key has been set as specified under [Requirements](#).

**Option 1:** Prevent Captive Portal Detection (VPN Portal Only) for Windows  
The zones.vpn file can be modified through the appliance CLI.

Add the following domains to **/bsc/siteConfiguration/named/zones.vpn**:

```
msftconnecttest.com  
msedge.net  
c-msedge.net
```

**Option 2:** Prevent Captive Portal Detection (All Portals) for Windows

Add the following domains to the Allowed Domains List. For instructions on adding domains, see **Add a domain** in section [Allowed Domains](#) of the Administration Guide.

msftconnecttest.com

msedge.net

c-msedge.net

Proceed to [Validate](#).

# Validate

## Establish VPN Connection

Using the VPN client, establish a connection and verify the following:

1. Host is assigned an IP address from the ASA.
2. If Persistent Agent is installed and notifications have not been disabled, the message “Network restrictions have been applied for this device” is displayed.
3. If an agent is not already installed, host is prompted to download the agent specified in the appropriate VPN Endpoint Compliance Policy. If the VPN user's session has been set up, and the user opens a browser and gets the wrong portal page (e.g., the normal Registration page rather than the VPN portal page), see [Address VPN Connection Delays](#).
4. If agent is installed, the appropriate scan configured in the VPN Endpoint Compliance Policy is run.
5. Once the scan completes and passes, host is granted access to the appropriate network.
6. If Persistent Agent is installed and notifications have not been disabled, the message “Network restrictions have been lifted for this device” is displayed.
7. Navigate to **Network > Inventory**.
8. The ports tab for the ASA model should display the user connected along with the adapter information below.

The screenshot shows the FortiNAC Lab interface. The left sidebar contains a tree view with categories like FortiNAC Lab, Branch Office, Concorc Office, Corporate Network, and various FGT, FSW, and PU421E3X1600547 AP-Us. The main panel is divided into two tabs: 'Ports' and 'Adapters'. The 'Ports' tab is active, showing a table with columns: Status, Device, Label, Name, Interface ID, IP Address, Connection State, Default VLAN, Current VLAN, Admin Status, Operational Status, Notes, Last Modified By, and Last Modified Date. Two rows are visible: one for 'ciscoasa.supportlab SupportGP' with IP 10.12.241.33 and 'Link Up' status, and another for 'ciscoasa.supportlab Testing' with IP 10.12.241.33 and 'Not Connected' status. Below the table are options to export, select all, or hide details. The 'Adapters' tab is also visible, showing a table with columns: Status, Host Status, IP Address, Physical Address, All IPs, Location, Connected Container, Media, Access Value, Vendor Name, Host Name, Operating System, Registered To, Logged On User, Persistent Agent, and Host Created. One row is visible for a Dell Inc. adapter with IP 172.16.197.10 and 'Link Up' status.

Status	Device	Label	Name	Interface ID	IP Address	Connection State	Default VLAN	Current VLAN	Admin Status	Operational Status	Notes	Last Modified By	Last Modified Date
Link Up	ciscoasa.supportlab	SupportGP	ciscoasa.supportlab SupportGP	10009	10.12.241.33	Link Up	SupportGP	SupportGP	On	Link Up		SYSTEM	05/27/20 05:06 PM EDT
Not Connected	ciscoasa.supportlab	Testing	ciscoasa.supportlab Testing	10009	10.12.241.33	Not Connected	Testing	Testing	On	Link Up		SYSTEM	05/27/20 02:31 PM EDT

Status	Host Status	IP Address	Physical Address	All IPs	Location	Connected Container	Media	Access Value	Vendor Name	Host Name	Operating System	Registered To	Logged On User	Persistent Agent	Host Created
Link Up	Link Up	172.16.197.10	28:F1:9E:3D:BE:51	10.12.240.34 (IPv4)	ciscoasa.supportlab SupportGP	Corporate Network	Wired	SupportGP	Dell Inc.	DESKTOP-KUJZSUJ	Windows 10 Pro 6.3 19H3		vpuser2	✓	05/27/20 05:04 PM EDT

## Ports

Label: Group Policy

Default VLAN: (Default Tunnel Group Policy)

Current VLAN: (Current Tunnel Group Policy)

## Adapters

IP Address: VPN IP Address

MAC address

Access Value: Assigned Group Policy

## View VPN Hosts

When hosts connect through a VPN device managed by FortiNAC, they may or may not be modeled as FortiNAC hosts. If a FortiNAC agent running on the remote machine has not identified the machine to FortiNAC, then that machine cannot be identified as a host in FortiNAC. Connected hosts can be viewed by selecting the VPN User Table option available from the device specific menu. Enter information into the filter fields to narrow the results and locate specific hosts.

1. Click **Network > Inventory**.
2. Right click on the ASA device model and click **VPN User Table**.

A list of the connected VPN hosts is displayed. VPN users can be filtered by any combination the following fields: User Name, MAC Address, IP Address, Session ID, Group or Protocol.

The screenshot shows the FortiNAC-VM-CA VPN Users interface. At the top, there is a navigation bar with tabs: Bookmarks, Users, Hosts, Network Devices, Logs, Policy, System, and Help. Below the navigation bar, there is a section titled "Filter VPN Users" with input fields for User Name, MAC Address, IP Address, Session ID, Group, and Protocol. An "Apply" button is located below these fields. Below the filter section, it says "One item found. 1". Below this, there is a table with one row of data. The table has columns for User Name, MAC Address, IP Address, Session ID, Group, and Protocol. The data row shows: vpnuser2, 28:F1:0E:3D:BE:01, 172.16.197.13, 109, SupportGP, and AnyConnect-Parent SSL-Tunnel DTLS-Tunnel.

User Name	MAC Address	IP Address	Session ID	Group	Protocol
vpnuser2	28:F1:0E:3D:BE:01	172.16.197.13	109	SupportGP	AnyConnect-Parent SSL-Tunnel DTLS-Tunnel

# Troubleshooting

If you are experiencing problems with the VPN device and users managed by FortiNAC, check the following:

1. Static route(s) are defined to send traffic to FortiNAC from the VPN device.
2. An IP pool has been configured on the ASA or an IP helper is configured to point to an external DHCP server for VPN.
3. SNMP read/write community strings are setup on the VPN device to facilitate device discovery.
4. Privileged administrator account is used when creating the device model in FortiNAC. The VPN device restricts command line access to all other accounts.
5. Telnet or SSH is enabled on the VPN device.
6. The FortiNAC Server or Control Server should always be able to communicate via SSH or Telnet to control connecting hosts.
7. ACLs and routes are defined to allow users on both restricted and non-restricted networks to access the FortiNAC VPN interface.

## Communication Using Virtual IP (VIP) in L2 High Availability Configurations

Hosts from the VPN address pool are unable to communicate with the FortiNAC VIP once the script is run. This primarily affects Administration UI access and Persistent Agent communication depending upon configuration.

### Administration UI Access

1. In the Primary Control Server CLI, review the `/etc/hosts` file. Type  
**cat /etc/hosts**
2. If the `/etc/hosts` file has the “nac” entry on the same line as the VIP (example below), then it will be necessary to modify the file.  
`192.168.8.25 oak.mynetworks.com oak cm nac`
3. Modify `/etc/hosts` and remove “nac” from the line and save.  
`192.168.8.25 oak.bradfordnetworks.com oak cm`
4. Restart tomcat-admin service to apply changes:  
**service tomcat-admin restart**

### Persistent Agent Communication

Agents using the shared IP address or name as Allowed Servers (instead of the actual IP or name) are unable to communicate.

**Solution:** Use the primary and secondary FortiNAC Server/Application Server Fully Qualified Domain Names (not the Shared name). See section **Persistent Agent Settings** in the [Persistent Agent Configuration and Deployment](#) reference manual for details.

## Related KB Articles

[Troubleshooting Cisco ASA VPN integrations](#)

## Debugging

Use the following KB article to gather the appropriate logs using the debugs below.

[Gather logs for debugging and troubleshooting](#)

**Note:** Debugs disable automatically upon restart of FortiNAC control and management processes.

Function	Syntax	Log File
RADIUS Authentication activity	<code>nacdebug -name RadiusManager true</code>	<code>/bsc/logs/output.master</code>
LDAP synchronization and lookup	<code>nacdebug -name DirectoryManager true</code>	<code>/bsc/logs/output.master</code>
SSH/Telnet CLI activity	<code>nacdebug -name TelnetServer true</code>	<code>/bsc/logs/output.master</code>
SNMP activity	<code>nacdebug -name SnmpV1 true</code>	<code>/bsc/logs/output.master</code>
Persistent Agent activity	<code>nacdebug -name PersistentAgent true</code>	<code>/bsc/logs/output.nessus</code>
Dissolvable Agent activity	<code>nacdebug -name AgentServer true</code>	<code>/bsc/logs/output.nessus</code>
Syslog activity	<code>nacdebug -name SyslogServer true</code>	<code>/bsc/logs/output.master</code>
VPN activity	<code>nacdebug -name RemoteAccess true</code>	<code>/bsc/logs/output.master</code>
Cisco ASA specific activity	<code>nacdebug -name CiscoASA true</code>	<code>/bsc/logs/output.master</code>
Disable debug	<code>nacdebug -name &lt;debug name&gt; false</code>	N/A

# Appendix

## How It Works

FortiNAC controls network access by managing a Network Object Group within the ASA. Access is restricted through the use of a NAC specific ACL applied to the IP addresses contained within that “Restricted” Network Object Group. In order to accomplish this, FortiNAC must use the below components to associate the device’s IP address and MAC address with the remote user.

### Session Data Components

- **User ID** (collected syslog and stored in FortiNAC database within the User record)
- **Remote IP address for the remote user connection** (collected via syslog and from the FortiNAC agent)
- **Device IP & MAC address** (collected via FortiNAC agent)

### FortiNAC Modeling of the ASA

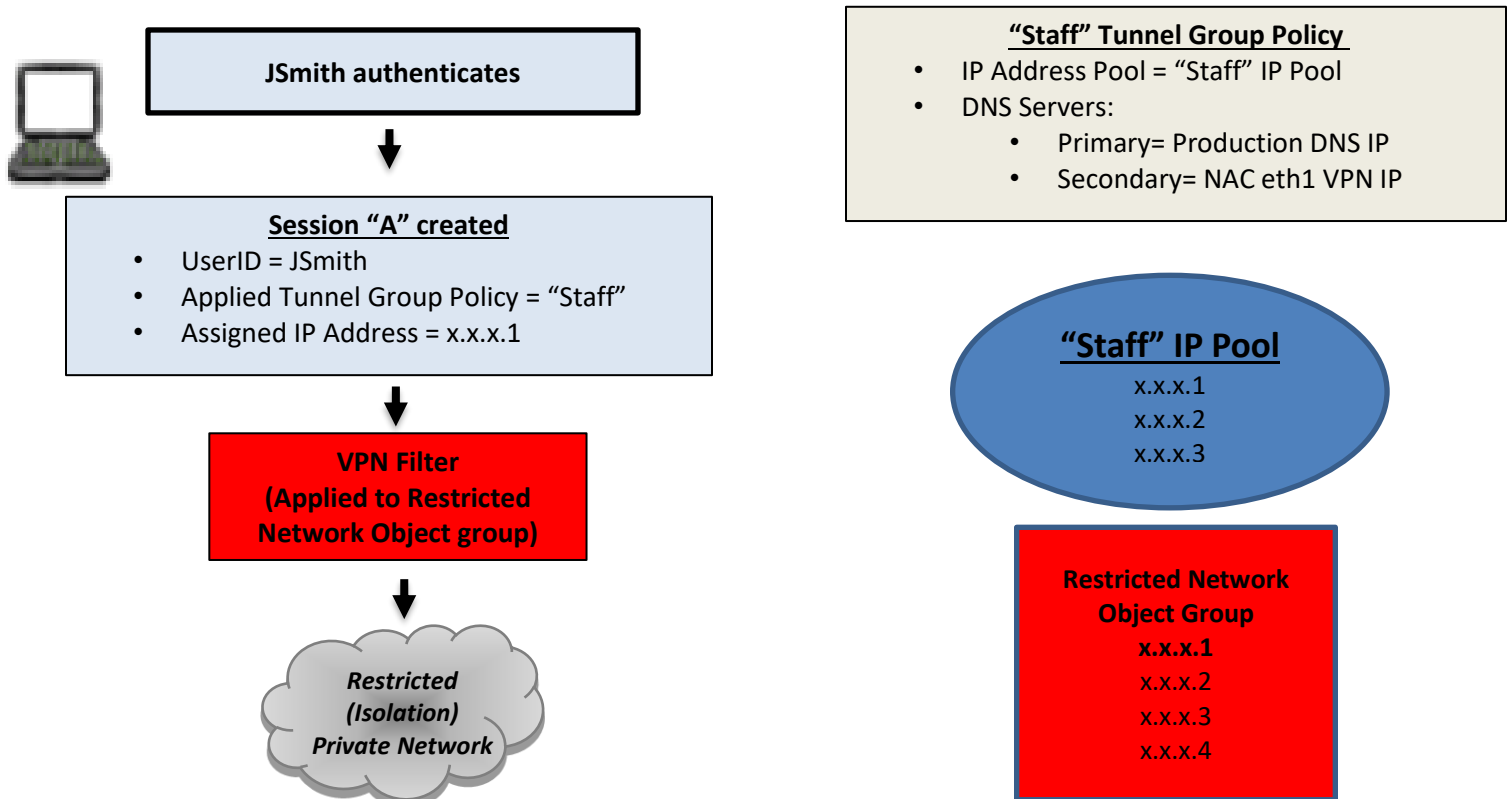
In order for the ASA VPN sessions to be managed by FortiNAC, the ASA must be modeled in Topology. This enables the following to operate properly:

- Syslog
- Agent communication
- CLI communication
- Identification of the VPN tunnels to be managed by FortiNAC



The following occurs when a device connects to a VPN managed by FortiNAC:

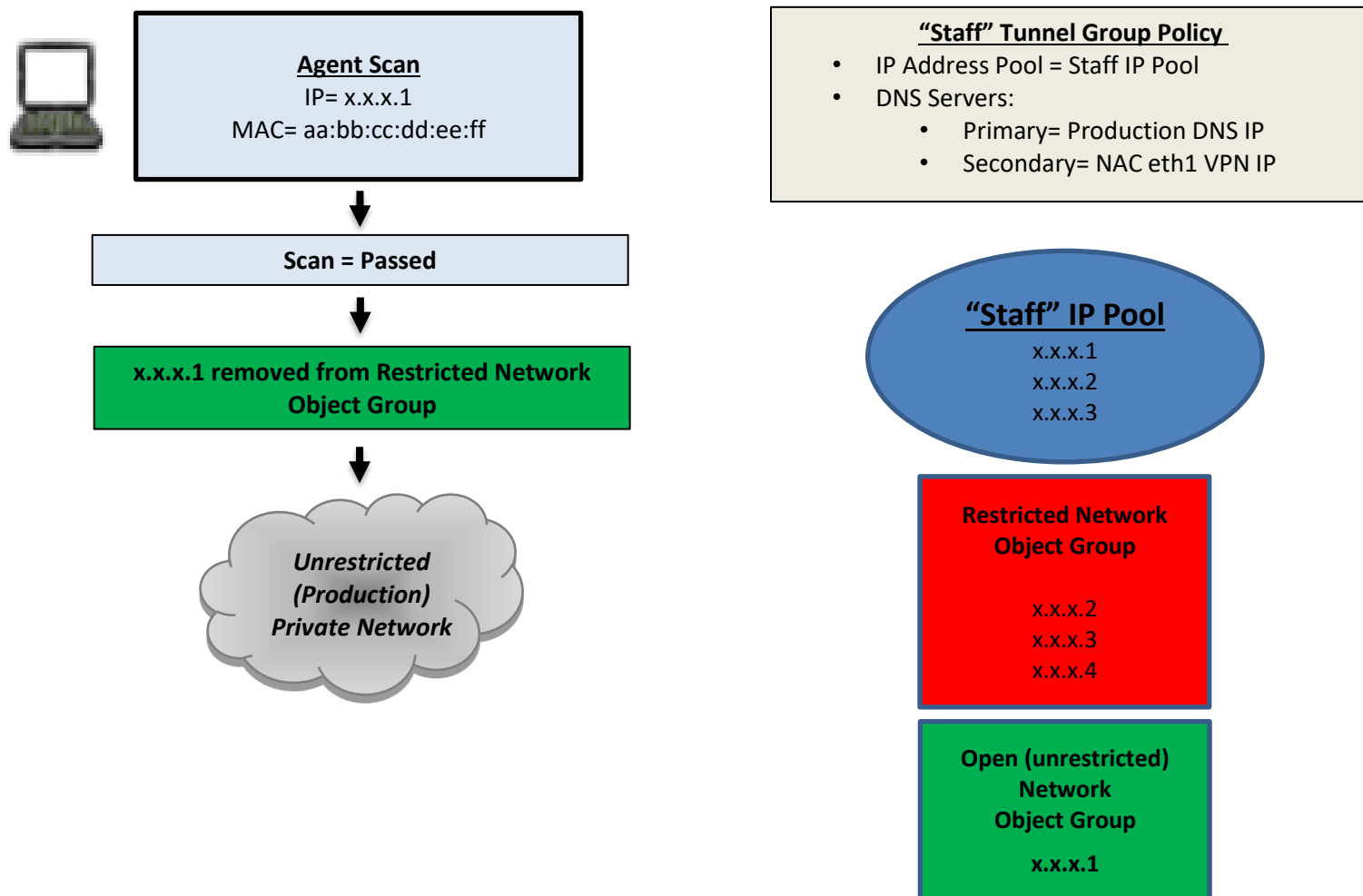
1. The remote user authenticates using either IPSec or SSL VPN client processes.
2. If authentication is successful, ASA creates session for user and sends syslog to notify NAC. Syslog contains the following:
  - User ID
  - Name of Tunnel Group Policy applied to user
  - IP address assigned from the IP Pool defined in the applied Tunnel Group Policy
  - Session ID the ASA built for the remote connection
3. Since the assigned IP address is contained within the Network Object Group by default, the NAC ACL restricts access.



- Upon isolation, the user is redirected to the appropriate VPN portal page.

**Note:** Until a FortiNAC agent executes, all VPN sessions that satisfy the ACL created for containment remain isolated. Devices that sense captive networks may trigger browsers while restricted.

- FortiNAC Agent scans device to evaluate posture.
- If scan passes, the device is granted production network access by removing the IP address from the Restricted Network Object Group (releasing associated ACL restrictions) and moving it to an “unrestricted” Network Object Group.



- On disconnect, ASA sends syslog to notify NAC of session termination
- IP address is added back to the Restricted Network Object Group, making address available for a new connection

## DNS File Entry Descriptions

`/var/named/chroot/etc/domain.zone.vpn` is used for managing DNS SRV records for agent communications over all VPN tunnels. There is a `domain.zone.*` file for each FortiNAC Service interface (Isolation, Registration, Remediation, etc). For more details, see [DNS Server Configuration](#) in the Administration Guide.

```
> cat /var/named/chroot/etc/domain.zone.vpn
```

```
<...>
```

```
$ORIGIN example.com.
```

```
b._dns-sd._udp PTR @
```

```
lb._dns-sd._udp PTR @
```

```
_networksentry._tcp PTR AgentConfig._networksentry._tcp
```

```
;Insert agent line here
```

```
; Needs to be here for BN_OTHER_HOSTNAME
```

```
AgentConfig._networksentry._tcp SRV 0 0 443 servername.domainname.com. << Mobile Agent SRV response*
```

```
                                TXT path=/vpn/agent/config
```

```
_networksentry._tcp  
SRV response*
```

```
SRV 0 0 443 servername.domainname.com. << Dissolvable Agent
```

```
                                TXT path=/vpn/agent/config
```

```
_bradfordagent._udp  
SRV response*
```

```
SRV 0 0 4567 servername.domainname.com. << Persistent Agent
```

```
_bradfordagent._tcp  
SRV response*
```

```
SRV 0 0 4568 servername.domainname.com. << Persistent Agent
```

```
*.example.com. IN A 172.16.99.6
```

```
;*.example.com. IN AAAA BN_VPN_6IP
```

\*Portal SSL Fully-Qualified Host Name configured in the UI under **Portal > Portal SSL**.

Example using Dissolvable Agent:

1. VPN isolation interface is configured and DHCP scope created with domain **example.com**.
2. Configuration Wizard writes **example.com** to the **\$ORIGIN** entry in **domain.zone.vpn** file
3. Endpoint connects to VPN tunnel and obtains DHCP information from VPN SERVER
4. Dissolvable Agent is downloaded from the Captive Portal and run
5. Agent sends SRV query for **\_networksentry.\_tcp.example.com**
6. Upon receipt of query, FNAC searches the `domain.zone.*` files for a matching domain in the **\$ORIGIN** entry
7. Since domain **example.com** matches the entry in **domain.zone.vpn**, FNAC responds to

the query with the priority (**0 0**), port (**443**) and server name (**servername.domainname.com**) as specified in the **\_networksentry.\_tcp** entry

8. Dissolvable Agent performs certificate check comparing **servername.domainname.com** to the Portal SSL Certificate securing **servername.domainname.com**

# Policy Based Routing

## Why it is Needed

Because VPN client IP addresses do not change when the network access changes, it is possible for traffic between agent and FNAC to drop due to asymmetric routes. By default, CentOS 7 drops asymmetrically routed packets before they leave the interface. If asymmetric traffic were to be allowed to transmit, the packet would most likely be dropped within the network.

Example 1:

Default route = eth0

Resulting behavior:

- Restricted (isolated) host communication over VPN would ingress **eth1** and egress **eth0**, resulting in an asymmetric route.
- Non-restricted (production) host communication over VPN would ingress eth0 and egress eth0.

Example 2:

Default route = eth0

Static route = eth1 for VPN network

Resulting behavior:

- Restricted (isolated) host communication over VPN would ingress eth1 and egress eth1
- Non-restricted (production) host communication over VPN would ingress **eth0** and egress **eth1**, resulting in an asymmetric route.

Policy Based Routing is used to ensure FNAC responds to inbound traffic using the interface from which it was received.

## How it Does it

Using a script, individual route tables are built for each FNAC interface (eth0, eth1, eth1:1, eth1:2, etc.). Each table contains routes for various networks to be used by the eth interface. If a packet is received on an interface, FNAC first looks for a route containing the source IP's network in the individual table. If no route for that network is found, FNAC looks at the main route table. IP rules determine the order used to lookup the tables.

Example:

### Main Route Table

Destination	Gateway	Mask	Interface
0.0.0.0	10.10.200.1	0.0.0.0	Eth0
10.10.18.0	10.10.201.129	255.255.255.0	Eth1
10.10.19.0	10.10.201.129	255.255.255.0	Eth1:1

### Eth0 Route Table

Destination	Gateway	Mask	Interface
0.0.0.0	10.10.200.1	0.0.0.0	Eth0
10.10.18.0	10.10.200.1	255.255.255.0	Eth0
10.10.19.0	10.10.200.1	255.255.255.0	Eth0

### Eth1 Route Table

Destination	Gateway	Mask	Interface
0.0.0.0	10.10.201.129	0.0.0.0	Eth1
10.10.18.0	10.10.201.129	255.255.255.0	Eth1
10.10.19.0	10.10.201.129	255.255.255.0	Eth1

### Eth1:1 Route Table

Destination	Gateway	Mask	Interface
0.0.0.0	10.10.201.129	0.0.0.0	Eth1:1
10.10.18.0	10.10.201.129	255.255.255.0	Eth1:1
10.10.19.0	10.10.201.129	255.255.255.0	Eth1:1

The files containing the route tables and ip rules for each configured interface are written to **/etc/sysconfig/network-scripts/**

Route files:

**route-eth0**

**route-eth1**

**route-eth1:1**

Example

```
> cat route-eth0
```

```
default via 10.10.200.1 dev eth0 src 10.10.200.147 table eth0
```

```
10.10.200.0/24 dev eth0 proto kernel scope link src 10.10.200.147 table eth0
```

Rule files:

**rule-eth0**

**rule-eth1**

**rule-eth1:1**

Example

```
> cat rule-eth0
```

```
from 10.10.200.147 lookup eth0 prio 10
```

## Other Commands

Display IP rules in effect and the order in which route tables will be read

**ip rule show**

Display routing table for a specific interface (table name = interface name)

**ip route show table <table name>**

Example: `ip route show table eth1`

## Modifying or Adding Interfaces After Script Has Run

1. Run the script. Type **setupAdvancedRoute**
2. Type **U** to uninstall
3. Once uninstalled, re-run the script. Type **setupAdvancedRoute**
4. Type **I** to install
5. Once script completes, verify configuration. Type **ip rule show**

There should now be a rule listed for each interface and sub-interface configured:

```
0: from all lookup local
10: from <eth0 IP address> lookup eth0
20: from <eth1 IP address> lookup eth1
30: from <eth1:1 IP address> lookup eth1:1
40: from <eth1:2 IP address> lookup eth1:2
32766: from all main
32767: from all default
```

Example:

```
>ip rule show
0: from all lookup local
10: from 10.200.20.20 lookup eth0
20: from 10.200.5.20 lookup eth1
30: from 10.200.5.21 lookup eth1:1
40: from 10.200.5.22 lookup eth1:2
32766: from all main
32767: from all default
```

6. Reboot appliance. Type **shutdownNAC**

*<wait 30 seconds>*

**shutdownNAC -kill  
reboot**

## Disable Persistent Agent Notifications

Login to the CLI as root and configure attributes specific to the Cisco ASA device model. Contact Support for assistance.

### All agent notifications when connecting over VPN

Disable: **device -ip <ASA\_IP> -setAttr -name DisableClientTransitionMessages -value true**

Re-enable: **device -ip <ASA\_IP> -setAttr -name DisableClientTransitionMessages -value false**

Example:

```
device -ip 192.168.1.1 -setAttr -name DisableClientTransitionMessages -value true
```

### “Network restrictions have been applied for this device” notification

Disable: **device -ip <ASA\_IP> -setAttr -name DisableRestrictMessageText -value true**

Re-enable: **device -ip <ASA\_IP> -setAttr -name DisableRestrictMessageText -value false**

### “Network restrictions have been lifted for this device” notification:

Disable: **device -ip <ASA\_IP> -setAttr -name DisableClearMessageText -value true**

Re-enable: **device -ip <ASA\_IP> -setAttr -name DisableClearMessageText -value false**



## Address VPN Connection Delays

If the VPN user's session has been set up, and the user opens a browser and gets the wrong portal page (e.g., the normal Registration page rather than the VPN portal page), follow this process. Also use this process to improve the host experience, where SSL VPN could cause a significant delay (from the time a VPN client connects, and downloads and installs the AnyConnect VPN Client).

The **remoteAccessDB.properties** file on the FortiNAC appliance contains the configuration for controlling remote access to your network. The **remoteAccessDB.properties** file is located in the following directory of the FortiNAC Server or Control Server:  
**/bsc/campusMgr/master\_loader/properties\_plugin**

Properties files stored in the **properties\_plugin** directory are overwritten during upgrades. Therefore, modifications to those files should be done in **.masterPropertyFile** which is never overwritten. Entries in the **.masterPropertyFile** file are written to the appropriate properties files when the FortiNAC software is restarted.

1. Login as root to FortiNAC Server or Control Server CLI.
2. Navigate to the **/bsc/campusMgr/master\_loader** directory.
3. Use an editor such as VI to open the **.masterPropertyFile** file.
4. At the top of the file there is a sample entry that is commented out. Follow the syntax of the sample entry to create your own changes. There are two attributes that can be modified, Idle time and read attempts. The example shown below contains the defaults. Increase the values as needed. Save the changes to the file.

```
FILE_NAME=./properties_plugin/remoteAccessDB.properties
{
com.bsc.plugin.remote.RemoteAccessServer.remoteArpIdleTime=10
com.bsc.plugin.remote.RemoteAccessServer.maxReadAttempts=12
}
```

**remoteArpIdleTime** – sets the time (in sec) to wait before processing an ARP request from the ASA looking for an IP address assignment for a newly authenticated user. The time between user authentication and IP address assignment can vary on the ASA depending on the type of VPN software being used on the remote client.

**maxReadAttempts** – Because the time it takes for a remote client to receive an IP from the ASA after authentication can be variable, it may exceed the configured **remoteArpIdleTime**. This value indicates how many subsequent attempts will be made to read the IP address from the device.

5. Restart FortiNAC using the following command:  
**restartCampusMgr**
6. From the CLI navigate to:  
**/bsc/campusMgr/master\_loader/properties\_plugin**
7. Display the contents of the **remoteAccessDB.properties** file to make sure the changes have been written correctly.

## ASA CLI Commands Used by FortiNAC

### Commands:

```
config t exit show arp
show running-config all tunnel-group | grep general-attri- utes
show running-config group-policy | grep internal
show vpn-sessiondb detail full remote | grep Session ID show vpn-sessiondb
detail full svc | grep Session ID terminal pager 0
network-object host
no network-object host object-group network
vpn-sessiondb logoff ipaddress <ip address> noconfirm
```

## Modifying IP List in Restricted Network Object Group

If the list of IP addresses is modified in the IP Pool and Restricted Network Object Group, FortiNAC must re-read the ASA in order to learn of the change. If this not done, endpoints assigned to the new IP addresses will not be redirected to the VPN Captive Portal page when connecting to the tunnel.

1. In the Administration UI, navigate to **Network Devices > Topology**
2. Right click on the ASA model and click **Resync Interfaces**.

## Disable Windows Browser Popups

**Note:** Only applicable to machines with Persistent Agent installed via GPO or software management program.

Disable browser popups on managed Windows machines (recommended). When configuring registry keys for Persistent Agent settings, include this key to disable popups:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NlaSvc\Parameters\Internet\EnableActiveProbing
```

Key Type: DWORD

Value: Decimal 0 (False)



**FORTINET®**



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.