FortiNAC

Cisco VPN ASA
Device Integration

Version: 8.3, 8.5, 8.6, 8.7, 8.8

Date: December 8, 2021

Rev: Q

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET KNOWLEDGE BASE

http://kb.fortinet.com

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

How It Works 6

Requirements 8

Considerations 9

Integration 10

Configure ASA 10

AAA Server Group 10

IP Pool 11

Open (Unrestricted) Network Object Group 11

Restricted Network Object Group 11

ACL 12

Tunnel Group Policy 14

Tunnel Group 15

Syslog 16

Configure FortiNAC 17

Isolation Interfaces 17

Policy Based Routes 19

Authentication Server Settings 21

Model ASA in Topology 21

Develop Default Endpoint Compliance Policy 23

Develop Network Access Policies (Optional) 25

Configure Captive Portal 27

Persistent Agent Configuration (Optional) 28

Disable Captive Network Assistant 29

Validate 31

Troubleshooting 33

Communication Using Virtual IP (VIP) in L2 High Availability Configurations 33

Related KB Articles 34

Debugging 34

Appendix 35

VPN Connection Process Details 35

DNS File Entry Descriptions 36
Policy Based Routing.. 38
Disable Persistent Agent Notifications... 41
Address VPN Connection Delays 42
ASA CLI Commands Used by FortiNAC 43
Modifying IP List in Restricted Network Object Group 43
Disable Windows Browser Popups... 43

Overview

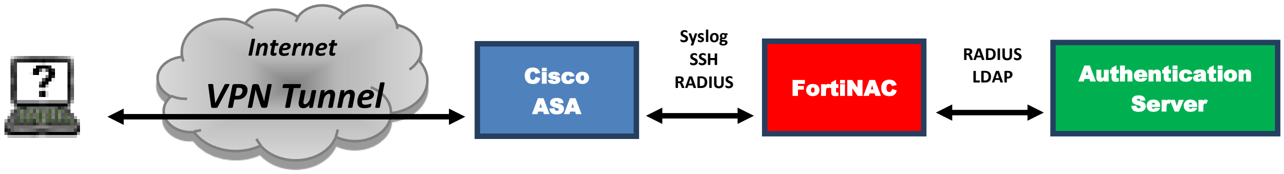
About this Document

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.

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 and classifies the device if it is unknown.

3. The device is evaluated by FortiNAC to verify its security posture.

4. If the device is considered to be safe, FortiNAC allows the device onto the network.

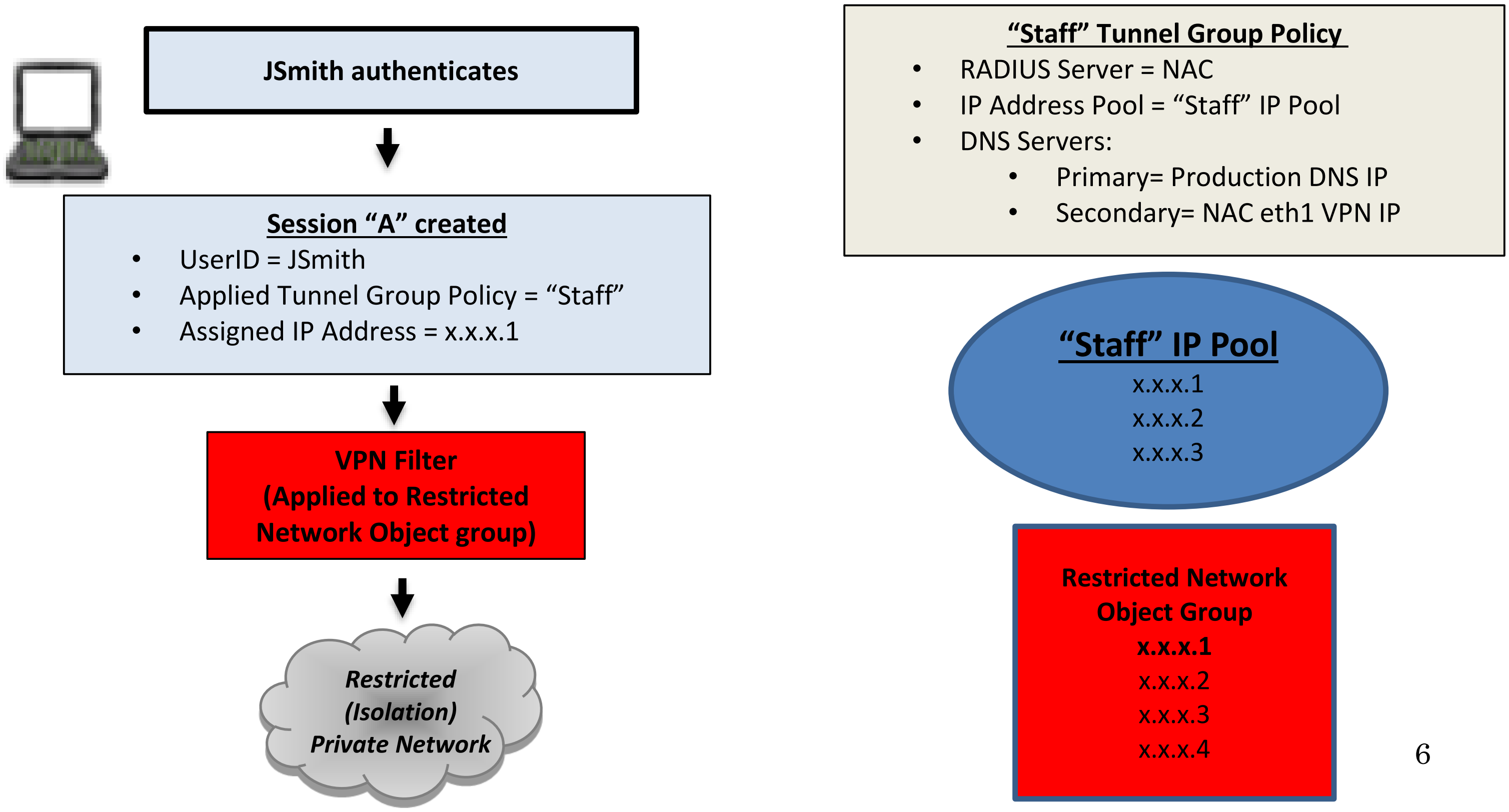
How It Works

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:

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

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

1. Remote user authenticates and ASA sends RADIUS to NAC (user ID is captured and stored in NAC database).
2. Once authentication completes, 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.



JSmith authenticates

Session “A” created

- UserID = JSmith
- Applied Tunnel Group Policy = “Staff”
- Assigned IP Address = x.x.x.1

VPN Filter (Applied to Restricted Network Object group)

Restricted (Isolation) Private Network

“Staff” Tunnel Group Policy

- RADIUS Server = NAC
- IP Address Pool = “Staff” IP Pool
- DNS Servers:
  - Primary= Production DNS IP
  - Secondary= NAC eth1 VPN IP

“Staff” IP Pool

x.x.x.1
x.x.x.2
x.x.x.3

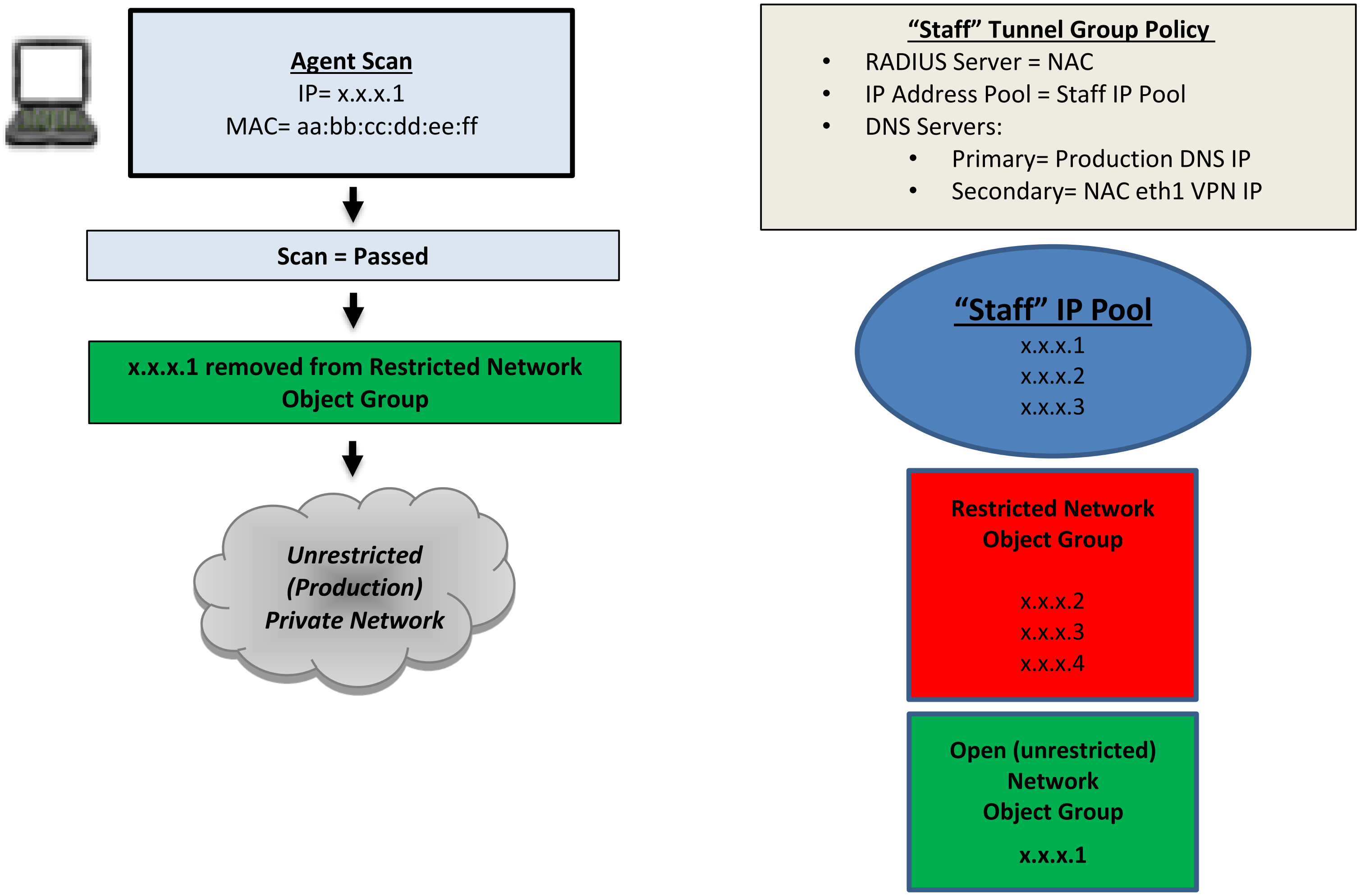
Restricted Network Object Group

x.x.x.1
x.x.x.2
x.x.x.3
x.x.x.4

4. 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.

5. FortiNAC Agent scans device to evaluate posture.
6. 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.


Agent Scan
IP= x.x.x.1
MAC= aa:bb:cc:dd:ee:ff
Scan = Passed
x.x.x.1 removed from Restricted Network Object Group
Unrestricted (Production) Private Network
"Staff" Tunnel Group Policy
RADIUS Server = NAC
IP Address Pool = Staff IP Pool
DNS Servers:
Primary= Production DNS IP
Secondary= NAC eth1 VPN IP
"Staff" IP Pool
x.x.x.1
x.x.x.2
x.x.x.3
Restricted Network Object Group
x.x.x.2
x.x.x.3
x.x.x.4
Open (unrestricted) Network Object Group
x.x.x.1

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

See VPN Connection Process Details in Appendix for additional information.

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.
- Remote user authentication using RADIUS. For detailed requirements, see section Configure ASA

Considerations

- Cisco ASA Cluster Mode is not supported at this time.
- IPv6 is not supported.
- **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.
- FortiNAC will pass through LDAP group policy attribute information from a 3rd party backend RADIUS server. This attribute provisions network access for VPN clients (bypasses the need for a FortiNAC Network Access 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

AAA Server Group

Configure a AAA server group defining FortiNAC as the RADIUS Server.

Protocol	RADIUS
RADIUS Server IP Address	FortiNAC eth0 IP address (Primary Server IP if High Availability configuration)
Secondary RADIUS Server IP Address	For High Availability FortiNAC configurations: Secondary Server FortiNAC eth0 IP address
Interface name	Interface with the IP address to be used for communication with FortiNAC.
Authentication Port	1812
Accounting Port	1813
RADIUS Secret (shared secret key)	Secret will also be used in FortiNAC ASA model configuration

Important: ASA

Commands:

```
aaa-server <name of RADIUS server Group> protocol radius
aaa-server <name of RADIUS server Group> <interface name> host <RADIUS
Server IP Address>
key <SHARED SECRET KEY>
authentication-port 1812
accounting-port 1813

##Add below lines if L2/L3 High Availability is configured##
aaa-server <name of RADIUS server Group> <interface name> host <Secondary
RADIUS Server IP Address>
key <SHARED SECRET KEY>
authentication-port 1812
accounting-port 1813
```

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

1. Create an object group for restricted access (restricted network object group).

   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.

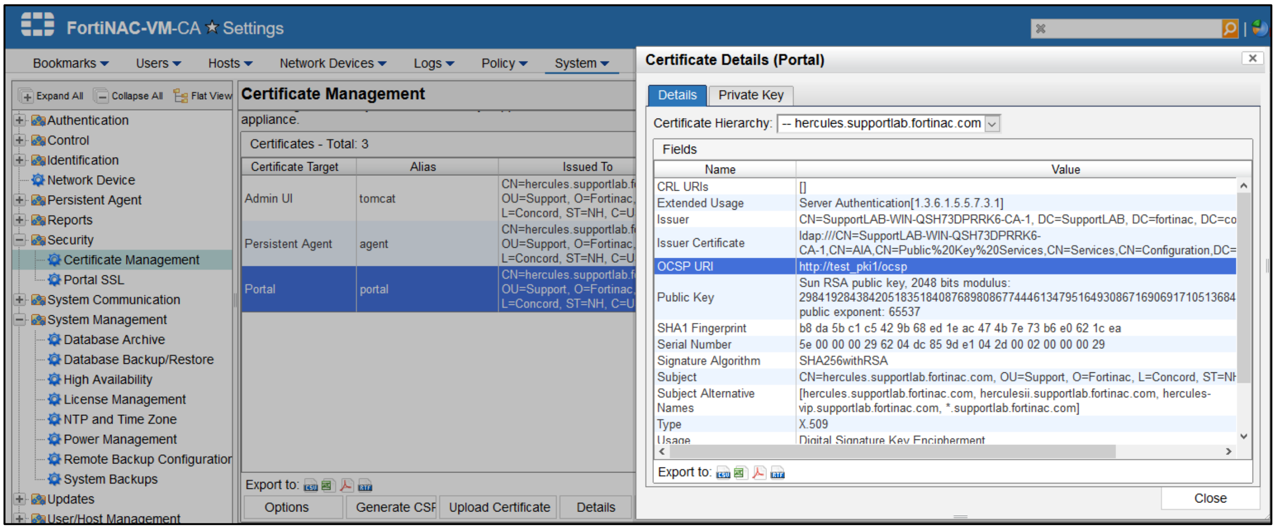
ACL

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 3rd 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 **System > Settings > Security > Certificate Management**.
2. Select the **Portal** target and click **Details**.
3. If using the Persistent Agent, select the **Persistent Agent** target and click **Details**.



Certificate Management

appliance.

Certificates - Total: 3

Certificate Target	Alias	Issued To

Admin UI	tomcat	CN=hercules.supportlab.f
		OU=Support, O=Fortinac,
		L=Concord, ST=NH, C=U

Persistent Agent	agent	CN=hercules.supportlab.f
		OU=Support, O=Fortinac,
		L=Concord, ST=NH, C=U

Portal	portal	CN=hercules.supportlab.f
		OU=Support, O=Fortinac,
		L=Concord, ST=NH, C=U

Certificate Details (Portal)

Certificate Hierarchy: -- hercules.supportlab.fortinac.com

Fields

Name	Value
CRL URIs	[]
Extended Usage	Server Authentication[1.3.6.1.5.5.7.3.1]
Issuer	CN=SupportLAB-WIN-QSH73DPRRK6-CA-1, DC=SupportLAB, DC=fortinac, DC=co
Issuer Certificate	ldap:///CN=SupportLAB-WIN-QSH73DPRRK6-CA-1,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=
OCSP URI	http://test_pki1/ocsp
Public Key	Sun RSA public key, 2048 bits modulus: 298419284384205183518408768980867744461347951649308671690691710513684 public exponent: 65537
SHA1 Fingerprint	b8 da 5b c1 c5 42 9b 68 ed 1e ac 47 4b 7e 73 b6 e0 62 1c ea
Serial Number	5e 00 00 00 29 62 04 dc 85 9d e1 04 2d 00 02 00 00 00 29
Signature Algorithm	SHA256withRSA
Subject	CN=hercules.supportlab.fortinac.com, OU=Support, O=Fortinac, L=Concord, ST=NH
Subject Alternative Names	[hercules.supportlab.fortinac.com, herculesii.supportlab.fortinac.com, hercules-vip.supportlab.fortinac.com, *.supportlab.fortinac.com]
Type	X.509
Usage	Digital Signature Key Encipherment

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. 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. FortiNAC must be set up as the RADIUS Server for that tunnel group on the VPN device.

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

Connecting using SSL: The default tunnel group must be configured to support remote RADIUS authentication using FortiNAC as the AAA server.

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.

Authenticating users via LDAP: Disable MSCHAP-v2 on ASA (otherwise, passwords will be unable to be decrypted).

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
authentication-server-group <name of RADIUS server group>
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 (RADIUS and back-end authentication)
- 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

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

3rd 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
Lease Pool Start	Starting IP address that delineates the range of IP addresses available to be managed by FortiNAC over the VPN tunnel. 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.
Lease Pool End	Ending IP address that delineates the range of IP addresses available to be managed by FortiNAC over the VPN tunnel. The VPN DHCP scope(s) must match the IP Pool (if configured) and the Restricted Network Object Group on the ASA.
Domain	Must match the domain value configured in the ASA. **NOTE**: • 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 **DNS File Entry Descriptions** in the Appendix for details. • OS X, iOS, and some Linux systems may have communication issues if a .local suffix is used.
Lease Time	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.

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

Note:

- Available in versions 8.6.4, 8.7.2 or higher.
- L2 Network Type configurations: Currently, Policy based routes do not work with L2 Network configurations.

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

To authenticate VPN network users, FortiNAC must have either a RADIUS server or a directory configured. If the desired authentication server is not already configured in FortiNAC, refer to the following sections of the **Administration Guide** in the Fortinet Document Library for instructions:

- **Configure RADIUS Settings**
- **Directories Configuration**
- **Portal Configuration/Content Fields/Global Properties**

Model ASA in Topology

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.

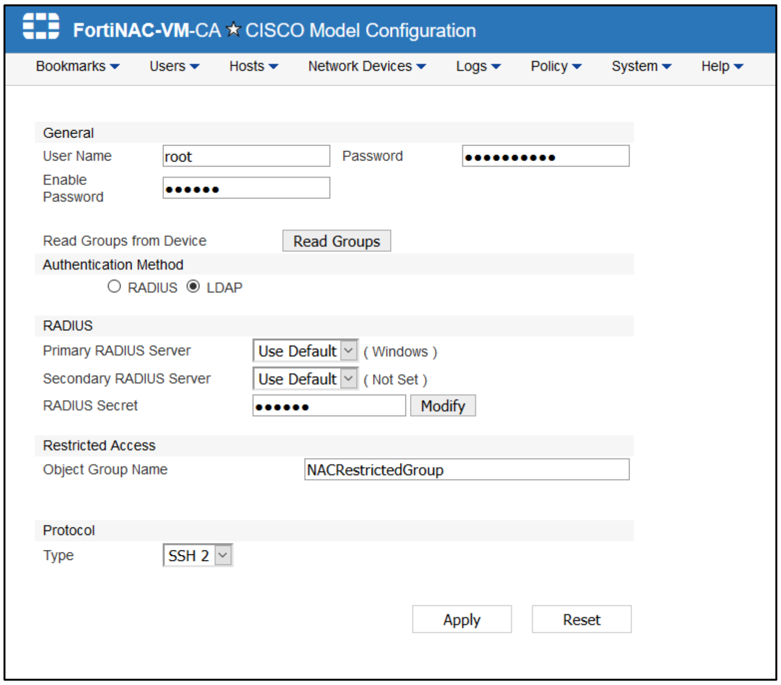
1. In the FNAC Administration UI, navigate to **Network Device > Topology.**
2. Model the ASA using the IP address from which RADIUS requests will be sent. See section **Add or modify a device** of the **Administration Guide** in the Fortinet Document Library for instructions.

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.

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
General	
User Name	The user id required for communication with the device.
Password	The password required to connect to the device.
Enable Password	The enable password for this device (required).
Read Groups	Connect to the device and read the group policy information into the FortiNAC database.
Protocol	
Type	Protocol used for connection to the device. Options are Telnet, SSH1, or SSH2
Authentication Method	
RADIUS **LDAP**	FortiNAC always receives a RADIUS request from the VPN. However, FortiNAC proxies that request either to a RADIUS server or an LDAP directory based on which option is selected here.
RADIUS	
Primary RADIUS Server	RADIUS server used for authenticating users connecting to the network through this device. Select the Use Default option from the drop-down list to use the server indicated in parentheses. Only valid if the authentication type is RADIUS.
Secondary RADIUS Server	If the primary RADIUS server fails to respond, this RADIUS server is used for authenticating users connecting to the network until the primary RADIUS Server responds. Select the Use Default option from the drop-down list to use the server indicated in parentheses. Only valid if the authentication type is RADIUS.
RADIUS Secret	Secret used for RADIUS authentication. This must match the RADIUS definition that you created for FortiNAC on the VPN device.
Restricted Access	
Object Group Name	Name of the Restricted Network Object Group configured in the ASA (case sensitive). **Important**: Name must exactly match.



General

User Name: root
Password: ●●●●●●●●●●●
Enable Password: ●●●●●●

Read Groups from Device

Authentication Method: ○ RADIUS ● LDAP

RADIUS

Primary RADIUS Server: Use Default (Windows)
Secondary RADIUS Server: Use Default (Not Set)
RADIUS Secret: ●●●●●●

Restricted Access

Object Group Name: NACRestrictedGroup

Protocol

Type: SSH 2

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

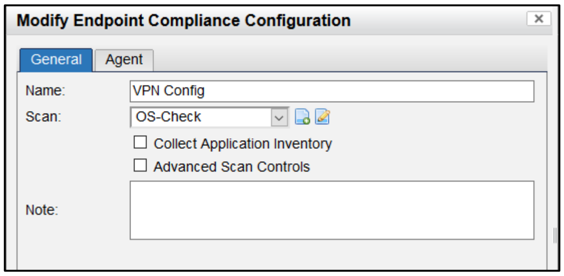
1. Navigate to **Policy > Policy Configuration**.
2. Under **Endpoint Compliance** click **Scans**.
3. Configure the scan to check for required programs and/or files. See section **Add or modify a scan** of the **Administration Guide** in the Fortinet Document Library for more information.

   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**.



Modify Endpoint Compliance Configuration

Name: VPN Config

Scan: OS-Check

☐ Collect Application Inventory

☐ Advanced Scan Controls

Note:

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:

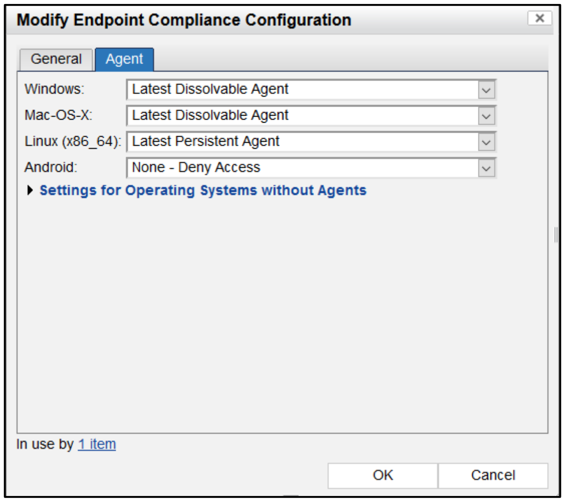
- **Persistent Agent (PA):** Installed on the user's PC and remains there, communicating with FortiNAC whenever the PC is on the network.

  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.

- **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.



Modify Endpoint Compliance Configuration

Windows: Latest Dissolvable Agent

Mac-OS-X: Latest Dissolvable Agent

Linux (x86_64): Latest Persistent Agent

Android: None - Deny Access

▸ Settings for Operating Systems without Agents

In use by 1 item

See section **Add or modify a configuration** of the **Administration Guide** for details for more details.

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 (*)>]

   Important: Do not include any other criteria when using the Dissolvable Agent. See related KB article for details.

2. Click **OK**.

See section **User/host profiles** of the **Administration Guide** for more information.

Create Endpoint Compliance Policy

Create the Endpoint Compliance policy using the User/Host Profile and Endpoint Compliance Configuration. Once created, adjust ranking as appropriate. See section **Add or Modify a policy** of the **Administration Guide** for details.

Develop Network Access Policies (Optional)

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

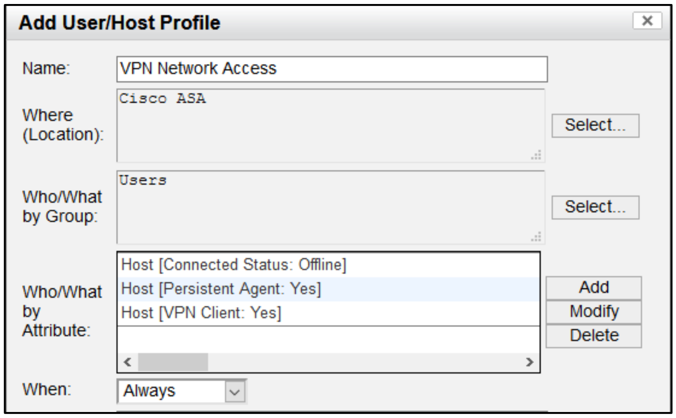
3. Create a separate **User/Host Profile** for each level of access (such as Staff and Executives):

    - 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: VPN Network Access

Where (Location): Cisco ASA

Who/What by Group: Users

Who/What by Attribute:
Host [Connected Status: Offline]
Host [Persistent Agent: Yes]
Host [VPN Client: Yes]

When: Always

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 section **Network Access Policies** of the **Administration Guide** in the Fortinet Document Library.

Configure 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
Index (Redirect)	Presented to user while NAC evaluates host to determine which page to display.
Download Page	The VPN Login page displayed to hosts that connect with user information available from the VPN device, but do not have an agent.
Profile Configuration Download	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.
Mobile Agent Download	A page presented to download the Agent from the relevant App store.
Instructions	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.
User Login (In-line only)	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.
Success	Host has successfully scanned and is released from isolation.

For more details, refer to section VPN Portal of the **Administration Guide** in the Fortinet Document Library.

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 section Portal Policies of the **Administration Guide** in the Fortinet Document Library.

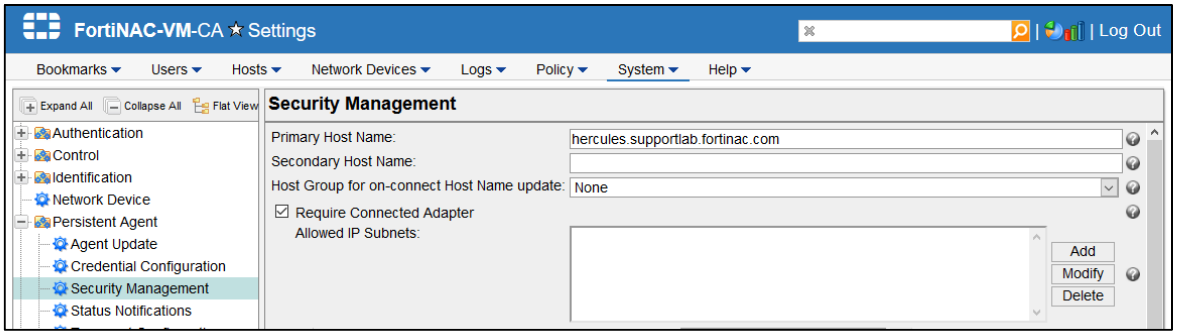
Persistent Agent Configuration (Optional)

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.



Security Management

Primary Host Name: hercules.supportlab.fortinac.com

Secondary Host Name:

Host Group for on-connect Host Name update: None

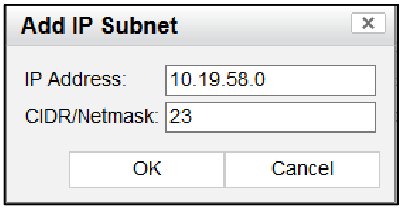
☑ Require Connected Adapter

Allowed IP Subnets:

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.



Add IP Subnet

IP Address: 10.19.58.0

CIDR/Netmask: 23

For more information regarding this option, refer to section Security Management of the **Administration Guide** in the Fortinet Document Library.

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** of the **Persistent Agent Deployment and Configuration** reference manual in the Fortinet Document Library.

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

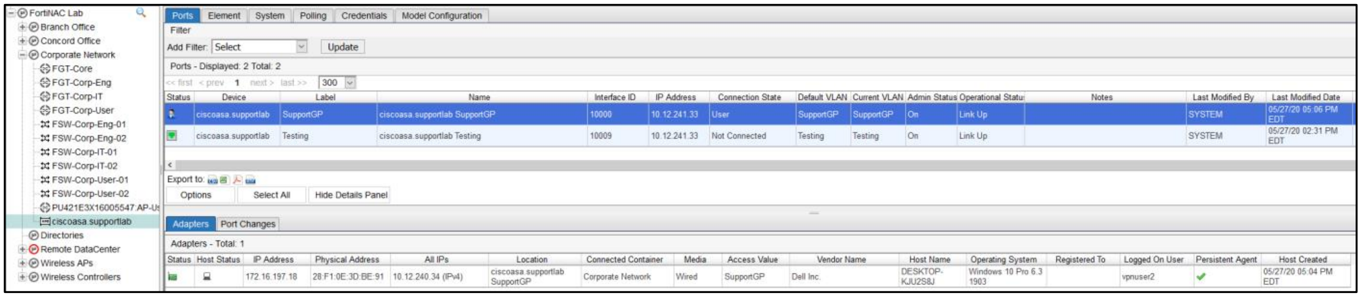
Proceed to Validate.

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 Devices > Topology.**
8. The ports tab for the ASA model should display the user connected along with the adapter information below.



Ports - Displayed: 2 Total: 2

Status	Device	Label	Name	Interface ID	IP Address	Connection State	Default VLAN	Current VLAN	Admin Status	Operational Statu	Notes	Last Modified By	Last Modified Date
	ciscoasa.supportlab	SupportGP	ciscoasa.supportlab SupportGP	10000	10.12.241.33	User	SupportGP	SupportGP	On	Link Up		SYSTEM	05/27/20 05:06 PM EDT
	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

Adapters - Total: 1

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
		172.16.197.18	28:F1:0E:3D:BE:91	10.12.240.34 (IPv4)	ciscoasa.supportlab SupportGP	Corporate Network	Wired	SupportGP	Dell Inc.	DESKTOP-KJU2S8J	Windows 10 Pro 6.3 1903		vpnuser2	✓	05/27/20 05:04 PM EDT

Ports
Label: Group Policy
Default VLAN: (Default Tunnel Group Policy)
Current VLAN: (Current Tunnel Group Policy)

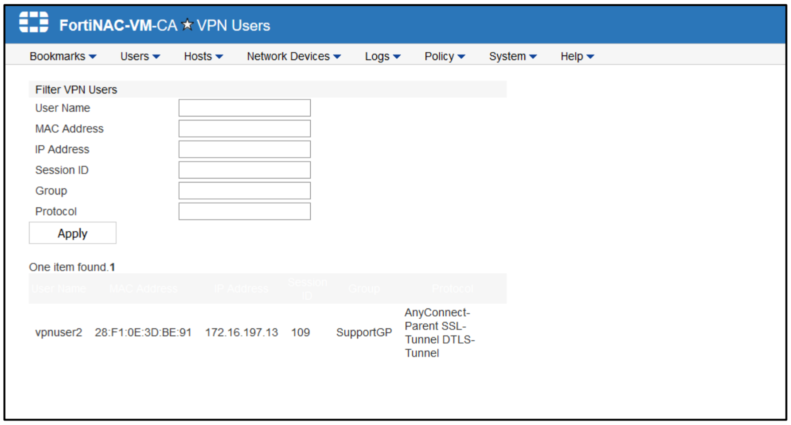
Adapters
IP Address: VPN IP Address
MAC address
Access Value: Assigned Group Policy

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 Devices > Topology**.
2. Expand the container icon where the VPN device is modeled and double-click the VPN device.
3. Select the device specific name, then click the **VPN User Table** option.

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.



Filter VPN Users

User Name

MAC Address

IP Address

Session ID

Group

Protocol

One item found.**1**

User Name	MAC Address	IP Address	Session ID	Group	Protocol
vpnuser2	28:F1:0E:3D:BE:91	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 RADIUS secret is the same on the VPN device, the FortiNAC RADIUS server configuration and the FortiNAC model configuration for the VPN device.
7. The FortiNAC Server or Control Server should always be able to communicate via SSH or Telnet to control connecting hosts.
8. 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). Refer to **Persistent Agent Deployment and Configuration** reference manual in the Document Library for details.

Related KB Articles

Troubleshooting Cisco ASA VPN integrations
RADIUS timeout during 2 Factor Authentication
Duo Two Factor Authentication with Cisco ASA VPN

Debugging

RADIUS activity:

```
CampusMgrDebug -name RadiusManager true
```

Cisco ASA specific:

```
CampusMgrDebug -name CiscoASA true
```

VPN activity

```
CampusMgrDebug -name RemoteAccess true
```

CLI activity

```
CampusMgrDebug -name TelnetServer true
```

Persistent Agent activity:

```
CampusMgrDebug -name PersistentAgent true
```

Dissolvable Agent activity:

```
CampusMgrDebug -name AgentServer true
```

Disable debugging:

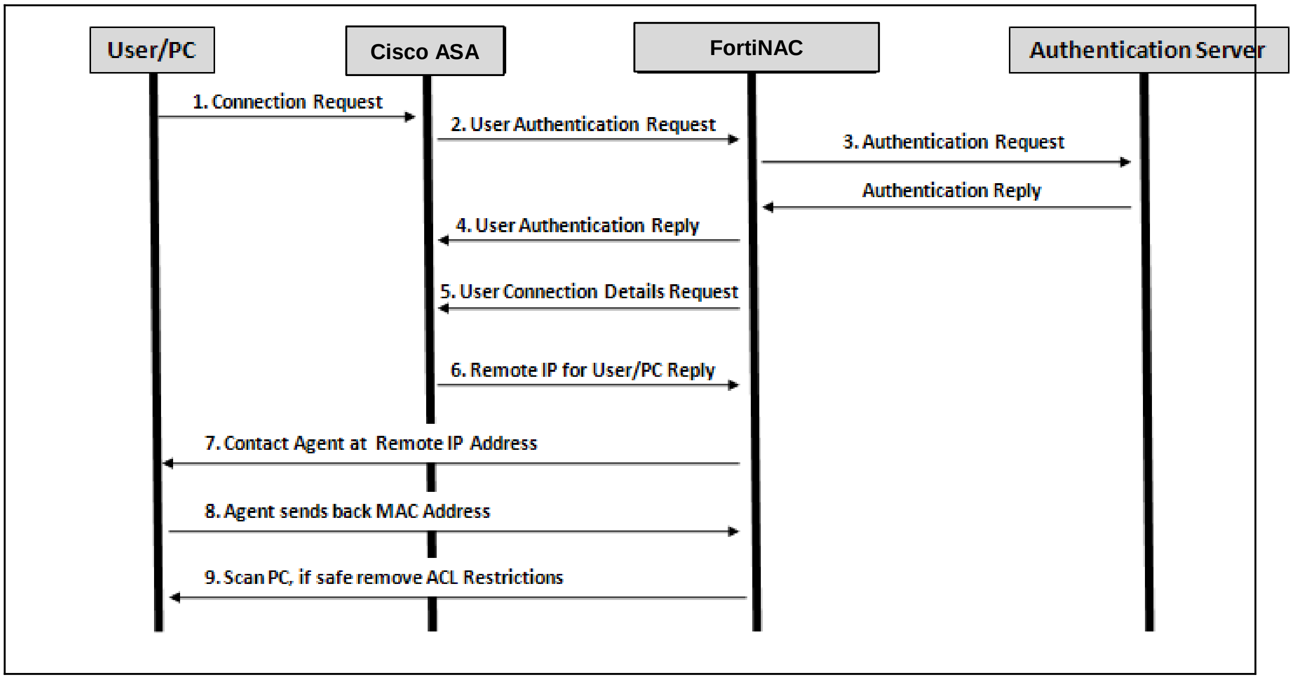
```
CampusMgrDebug -name <debug name> false
```

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

Appendix

VPN Connection Process Details

The following scenario describes the process for remote users that connect to the net- work through a Cisco ASA VPN when network access is controlled by FortiNAC.


User/PC
Cisco ASA
FortiNAC
Authentication Server
1. Connection Request
2. User Authentication Request
3. Authentication Request
Authentication Reply
4. User Authentication Reply
5. User Connection Details Request
6. Remote IP for User/PC Reply
7. Contact Agent at Remote IP Address
8. Agent sends back MAC Address
9. Scan PC, if safe remove ACL Restrictions

1. A user starts his VPN client or browses to the web page used for the VPN connection.
2. The user enters his user name and password. A connection request is sent to the VPN device.
3. The VPN device sends a RADIUS request to FortiNAC containing the user name of the connecting client and requests authentication.
4. Based on the option selected in the Model Configuration for the VPN device, FortiNAC proxies the request either to the RADIUS Server or the LDAP Server.
5. If the user is authenticated, FortiNAC returns a positive response to the VPN device and the user is allowed on the network. If configured, FortiNAC can respond with an alternate tunnel group policy as long as the IP pool from which the host is assigned an IP address is the same.
6. When the user is authenticated, the VPN device assigns the VPN connection an IP address, provides a DNS and imposes restrictions on the user's network access using an ACL configured as the VPN filter for the tunnel group policy. The ACL restricts the user's IP address from reaching anything other than FortiNAC and those sites designated by FortiNAC, such as a remediation site.

7. FortiNAC now knows who the user is and what the remote IP address is (syslog). The remote IP address is the tunnel IP address of the VPN connection.
8. If the user does not have an Persistent Agent installed, he is redirected to the captive portal. The user must download an agent. The administrator can provide either the Persistent Agent or the Dissolvable Agent
9. Once the user has an agent installed, the agent scans the user's PC and replies to FortiNAC with the MAC Address of the PC and the host state based on the scan.
10. If the user's PC does not pass the scan, he is redirected to a web page explaining why the scan failed. The user can correct the issue, such as having out of date virus definitions, and then rescan his PC. The user should disconnect from the VPN device and make corrections before reconnecting.
11. If the user passes the scan and is registered with FortiNAC, ACL restrictions are removed and the user can access the production network. Access restrictions are controlled based on the Tunnel Group or Tunnel Group policy.

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 0 0 443 servername.domainname.com.   << Dissolvable Agent
SRV response*
                                TXT path=/vpn/agent/config

_bradfordagent._udp             SRV 0 0 4567 servername.domainname.com.   << Persistent Agent
SRV response*
_bradfordagent._tcp             SRV 0 0 4568 servername.domainname.com.   << Persistent Agent
SRV response*

*.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 **System > Settings > Security > 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-attrib- 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)