



FortiNAC

FortiGate VPN Integration

Version: 8.7, 8.8

Date: December 16, 2021

Rev: S

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
How it Works	6
Requirements	9
Considerations.....	10
Integration	11
Configure FortiGate	11
System Administrator Account	11
REST API Administrator Account (Optional)	11
REST API.....	11
Address Objects.....	12
RADIUS Server.....	14
Syslog Settings.....	15
SSL VPN	17
IPSec VPN.....	20
Configure FortiNAC	22
Isolation Interfaces	22
Policy Based Routes	25
System Defined Uplink Count.....	26
Authentication Server Settings	26
Add Device Model	26
FortiGate Device Model Configuration	28
Logical Networks	29
Security Fabric Communication.....	29
Captive Portal	30
Persistent Agent Configuration.....	31
Disable Captive Network Assistant	32
Default Endpoint Compliance Policy (Optional)	33
Network Access Policies.....	36
Finalize Configuration	37
Establish Security Fabric Connection with FortiGate.....	37
Create User Group in FortiGate (Required for FortiOS versions prior to 6.2)	39

Create FortiGate Firewall Policies.....	40
Enable VPN Management for Existing FortiGate Models	43
Validate	44
Troubleshooting	45
Related KB Articles.....	45
Debugging.....	46
Appendix	47
VPN Connection Process Details	47
SSL VPN Settings (UI).....	48
DNS File Entry Descriptions	50
Policy Based Routing.....	52
Disable Persistent Agent Notifications.....	55
FSSO Groups on the SSL Interface (6.0.x Only)	55
ARP Data Collection Prioritization.....	57
Disable Windows Browser Popups.....	57

Overview

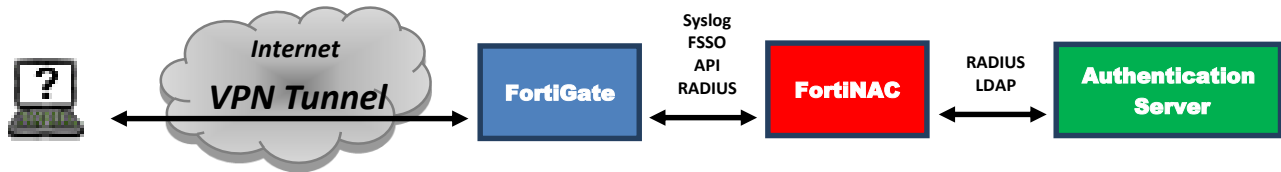
About this Document

The information in this document provides guidance for configuring the Fortinet FortiGate to support the management of VPN sessions by FortiNAC (FortiNAC). This document details the items that must be configured.

The intent of this document is to build new VPN configurations in order to allow any existing connections to continue working. Once the FortiNAC managed VPN has been tested, clients can be moved to the new tunnel.

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 user connects to the VPN tunnel, the device is restricted. 🚦
2. FortiNAC identifies the device as known and trusted. 🆔
3. FortiNAC verifies the security posture. 🔍
4. FSSO tags are sent to the FortiGate so the correct policy is matched and device is unrestricted. 🚦

How it Works

FortiNAC controls network access by leveraging Fortinet Single Sign-On (FSSO) on the Fortigate. Network access is restricted for VPN users by default when users connect. Access is only modified if the user successfully authenticates through FortiNAC, runs an appropriate FortiNAC agent and passes any required compliance checks. Once the user and host are identified and verified to be in compliance with the organization's prescribed policies, network access restrictions can be lifted. FortiNAC sends group and/or tag information to the FortiGate to adjust the user's network access according to the rules established in both FortiNAC and the FortiGate by the administrator.

Session Data Components

- **User ID** (collected via RADIUS, syslog and API from the FortiGate)
- **Remote IP address for the remote user connection** (collected via syslog and API from the FortiGate and from the FortiNAC agent)
- **Device IP and MAC address** (collected via FortiNAC agent)

FortiNAC Modeling of the FortiGate

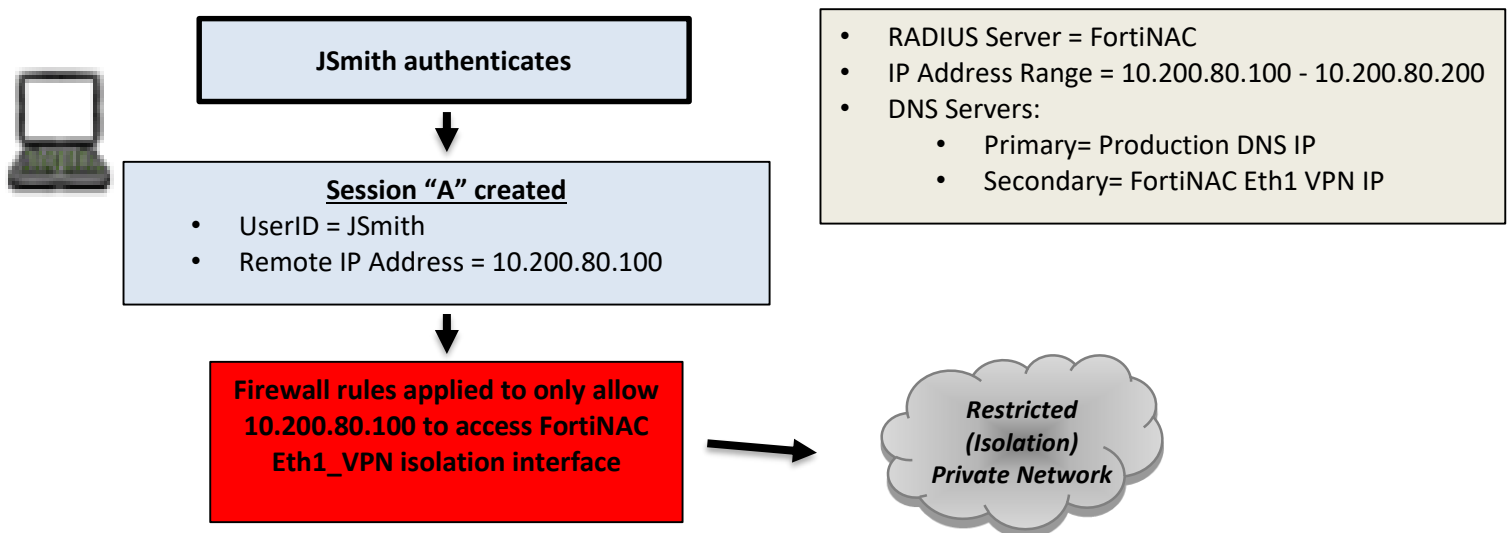
In order for the FortiGate VPN sessions to be managed by FortiNAC, the FortiGate must be modeled in Topology. This enables the following to operate properly:

- RADIUS
- Syslog
- Agent communication
- API communication
- FSSO
- Identification of the VPN tunnels to be managed by FortiNAC

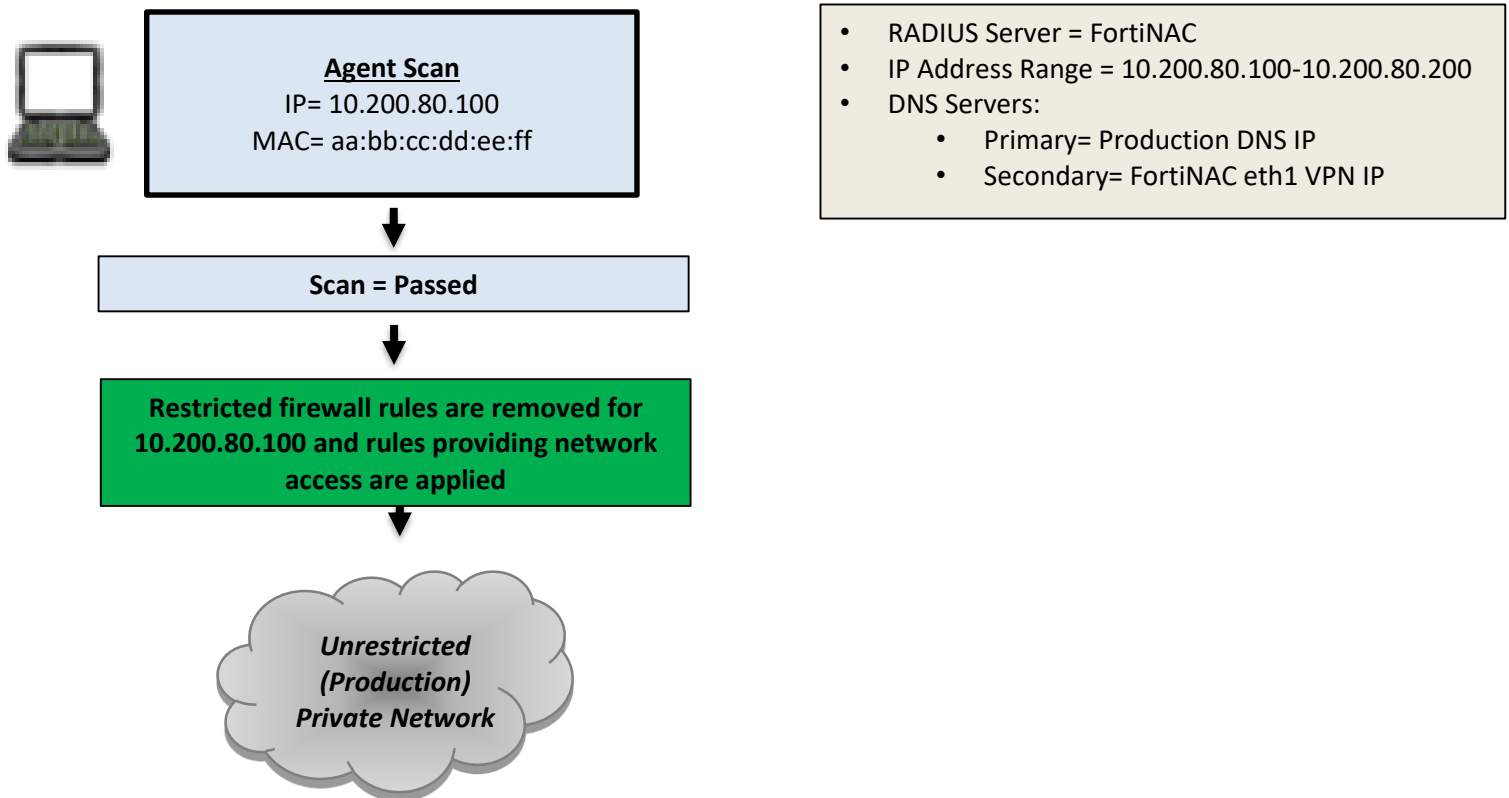
The following occurs when a device connects to a FortiGate VPN managed by FortiNAC:

1. The remote user authenticates using either IPSec or SSL VPN client processes.
2. FortiGate sends RADIUS authentication request to FortiNAC.
3. If authentication is successful, the FortiGate establishes a session and sends a syslog message to FortiNAC containing user, IP, and other session information.
4. FortiGate firewall rules exist to restrict all network access from the VPN interface and remote IP address range configured for VPN connections. The rules only allow access to FortiNAC isolation interface. DNS rules exist on the FortiNAC to resolve all queries to its isolation interface.
5. Devices without a FortiNAC agent: while restricted, all user HTTP requests are redirected to a VPN captive portal on FortiNAC. The portal page indicates that the user is currently restricted and, based upon administrator policy, can allow users to download and run a FortiNAC agent.

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



6. Once an FortiNAC agent executes and successfully communicates with the FortiGate, FortiNAC correlates information from the agent with data from the FortiGate to determine the host and adapter being used for the connection. It then updates the connection status of the host/adapter and triggers policy lookup and FSSO updates.
7. If the host/adapter is compliant with all necessary policies, FortiNAC tag/group information is sent to the FortiGate using FSSO which affects which FortiGate firewall rules control the session.
8. On disconnect, the FortiGate sends syslog to notify FortiNAC of session termination.
9. The host connection is terminated in FortiNAC which triggers FSSO to update the FortiGate to remove any tag/group information.
10. Default VPN firewall rules once again become effective.



Requirements

FortiNAC

- Supported Engine Version: 8.7.2 or greater
- Recommended Engine Version: 8.8.8, 9.1.2 or greater
- Remote device must have either the FortiNAC Dissolvable or Persistent Agent
 - Supported FortiNAC Agent Version: 5.2.3 or greater
 - Recommended FortiNAC Agent Version: 5.2.6
 - 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

FortiGate

- Supported Firmware Version: 6.0.5 or greater
- Recommended Firmware Version:
 - 6.2: 6.2.8 or greater
 - 7.0: (if using post-login banner) Requires FortiNAC [8.8.8](#), [9.1.2](#) or greater.
- SNMP community or account
- Administrator account
 - Visibility only: System read access to all VDOMs
 - Control: System read/write access to all VDOMs
- VPN tunnel cannot be configured to use DHCP relay

Considerations

- **NOTE:** When SSL VPN Settings are applied via the FortiGate UI, all existing SSL VPN connections are disconnected. Applying settings should be done during a Maintenance Window.
- **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.
- **FortiGate can only support one FSSO agent sending tags for a specific endpoint IP address.** If there are multiple agents, the FortiGate entries will be overwritten when other FSSO agents send information for the same endpoint IP. Therefore, the following should be done prior to integration:
 - Identify any other FSSO agents that provide logon information for the same endpoints FortiNAC would be managing through the FortiGate. For additional information, see section **Agent-based FSSO** in the FortiOS 6.0.0 Handbook (Tip: Open in New Tab):
<https://docs2.fortinet.com/document/fortigate/6.0.0/handbook/482937/agent-based-fsso>
 - For those agents, logon events must be blocked. See related KB article **Excluding IP addresses from FSSO logon events** (Tip: Open in New Tab):
<https://community.fortinet.com/t5/FortiGate/Technical-Tip-Excluding-IP-addresses-from-FSSO-logon-events/ta-p/196270>
 - Develop a plan to make the appropriate modifications to existing firewall policies to accommodate FortiNAC as the FSSO agent for the managed endpoint IP address scope.

Integration

Configure FortiGate

System Administrator Account

A System Administrator account is used for SSH and REST API access on the FortiGate. To create or view user accounts, navigate to **System > Administrators**.

REST API Administrator Account (Optional)

In FortiNAC version 8.8.3 and higher, a FortiGate REST API Administrator key can be used in addition to the System Administrator Account. The API key allows FortiNAC to bypass the need to authenticate every time it connects, improving performance.

1. Navigate to **System > Administrators**
2. Click **Create New > REST API Admin.**
3. Configure the settings using the table below

Username	
Comments	
Administrator Profile	(Read/Write access to all VDOM's)
Trusted Hosts	FortiNAC IP's to Trusted Hosts list (ip/mask)

4. Click **OK**. The New API key window opens.
5. Copy the key to the clipboard and click **Close**. Save the key for use in the FortiNAC configuration section.
6. Click **OK**.

REST API

REST API is required for communication with FortiNAC and must be configured. Verify the appropriate port is configured:

1. In the FortiGate UI, navigate to **System > Settings**.
2. Under **Administration Settings**, modify the **HTTPS port** as necessary (another service may already use 443).
3. Click **Apply** to save any modifications.

Address Objects

Via the UI or CLI, configure Address objects for the VPN IP addresses. **Note:** These addresses will be configured in FortiNAC Configuration Wizard and VPN Network Access Policies in later steps.

UI:

1. Navigate to **Policy & Objects > Addresses**
2. Select **Create New > Address**
3. Configure based on the entries in the table below. Click **OK** to save

Name	Address Object entry name
Type	IP Range
Subnet/IP Range	Enter the IP Addresses for Start and End of the lease pool range for the VPN scope. Examples: VPN DHCP range (SSL): 10.200.80.10-10.200.80.99 VPN DHCP range (IPSec): 10.200.80.100 – 10.200.80.200
Interface	Any
Show in address list	enabled

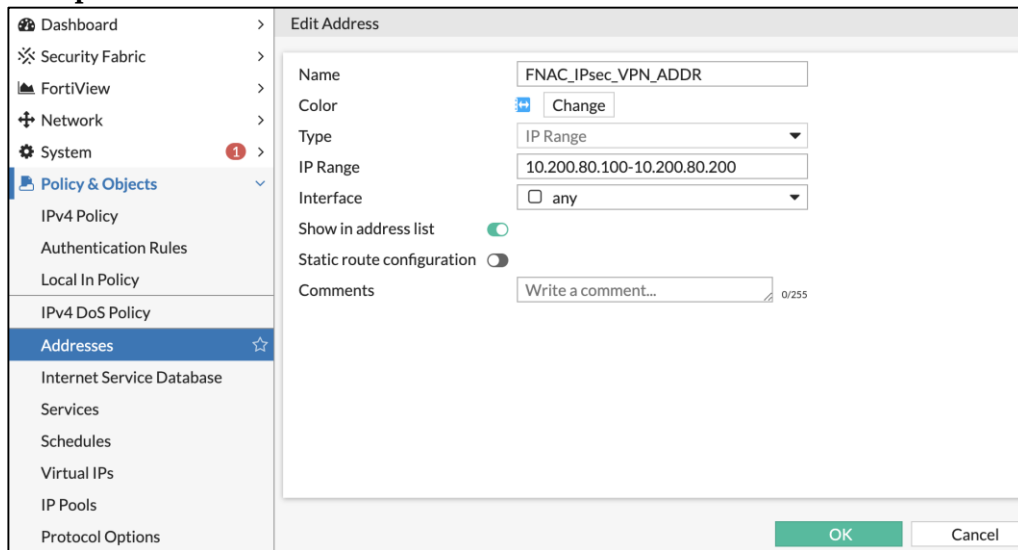
SSL UI Example

Name	Type	Details	Interface	Visibility	Ref.
Address 1/16					
FNAC_SSL_VPN_ADDR	IP Range	10.200.80.10 - 10.200.80.99		Visible	7

SSL CLI Example

```
config firewall address
    edit "FNAC_SSL_VPN_ADDR" << Address Object name
        set uuid 67dd7c4c-3143-51ea-6b02-828a306a7e68
        set type iprange << Type
        set color 7
        set start-ip 10.200.80.10 << Start of range
        set end-ip 10.200.80.99 << End of range
    next
end
```

IPSec UI Example



Name	Type	Details	Interface	Visibility	Ref.
Address 1/17					
FNAC_IPsec_VPN_ADDR	IP Range	10.200.80.100 - 10.200.80.200		Visible	7

IPSec CLI Example

```
config firewall address
    edit "FNAC_IPsec_VPN_ADDR" << Address Object name
        set uuid c27dd45c-4288-51ea-13c5-533055ae334b
        set type iprange << Type
        set color 18
        set start-ip 10.200.80.100 << Start of range
        set end-ip 10.200.80.200 << End of range
    next
end
```

RADIUS Server

Configure FortiGate to point RADIUS to FortiNAC when VPN clients connect.

Multiple VDOM/Split-Task VDOM: RADIUS settings must be configured for each VDOM sending RADIUS requests to FortiNAC.

UI:

1. Create a RADIUS server entry for FortiNAC. Navigate to **User & Device > RADIUS Servers**
2. Select **Create New**
3. Configure based on the entries in the table below. Click **OK** to save

Name	RADIUS Server entry name
Authentication Method	Default or Specify
NAS IP	Modeled IP of FortiGate in FortiNAC - IP address used to communicate with the RADIUS server and used as NAS-IP-Address and Called-Station-ID attributes.
Primary Server – IP/Name	FortiNAC eth0 IP address (Primary Server IP if High Availability configuration)
Primary Server – Secret	RADIUS secret (must match secret in FortiNAC model)
Secondary Server – IP/Name	For High Availability FortiNAC configurations: Secondary Server FortiNAC eth0 IP address
Secondary Server – Secret	For High Availability FortiNAC configurations: RADIUS secret (must match secret in FortiNAC model)
Source IP	(Configured in CLI only) Modeled IP of FortiGate in FortiNAC - Ensures the RADIUS packets are sourced from the IP address managed by FortiNAC. FortiNAC drops RADIUS traffic sourced from any device that is not modeled in Topology.

4. Create a User Group containing the FortiNAC RADIUS server entry. Navigate to **User & Device > User Groups**
5. Select **Create New**
6. Configure based on the entries in the table below:

Name	User Group Name
Type	Firewall

7. Under **Remote Groups** click **Add**
8. From Remote Server drill-down menu select the FortiNAC RADIUS server entry and click **OK**. Click **OK** again to save

UI Example

The screenshot shows the FortiGate web interface. On the left is a navigation sidebar with categories like Dashboard, Security Fabric, FortiView, Network, System, Policy & Objects, Security Profiles, VPN, and User & Device. Under 'User & Device', 'User Groups' is selected. The main panel is titled 'Edit User Group'. It contains a form with the following fields: 'Name' (FortiNAC RADIUS), 'Type' (Firewall), and 'Members' (a button with a plus sign). Below this is a 'Remote Groups' section with a table. The table has two columns: 'Remote Server' and 'Group Name'. There is one row with 'FortiNAC RADIUS' in the 'Remote Server' column. Above the table are buttons for '+ Add', 'Edit', and 'Delete'. At the bottom of the form are 'OK' and 'Cancel' buttons.

9. In CLI, add the source IP address

CLI Example

```
config user radius
```

```
    edit "FortiNAC RADIUS" << User group
```

```
        set server "10.200.20.20" << Primary FortiNAC Server eth0 IP
```

```
        set secret ENC
```

```
G30NVjYyxRX1alYvO19/bcaQG90sjqxMlyfprVqwn9TBFNZqf+sXazBPLW6w4KTgHTTGQwOZs6LA  
FLqPQjFJo6NSmuOUOqo+6JGgt1RE0mqg4aWp6AQGcKwnHsIOPiSJKwSf/hzVfbXN0Q8FdoVn/7fw
```

```
        set nas-ip "10.200.20.1" << IP of FortiGate model in FortiNAC
```

```
        set source-ip "10.200.20.1" << IP of FortiGate model in FortiNAC
```

```
    next
```

```
end
```

```
next
```

```
end
```

Syslog Settings

In the FortiGate CLI configure FortiNAC as a syslog server:

- Enable send logs to syslog
- Add the primary (Eth0) FortiNAC IP Address of the control server.
- **Important:** Source-IP setting must match IP address used to model the FortiGate in Topology
- Enable Event Logging and make sure that VPN activity event is selected.
- Log messages with ids of 0101039947 and 0101039948 (SSL), or 0101037129 and 0101037134 (IPSec) must be sent to FortiNAC.

Note: Care should be taken to avoid having the FortiGate send too many unnecessary log messages to FortiNAC. This can cause delays in message processing or even loss of messages.

CLI Settings:

FortiOS below 7.0

```
config log syslogd setting
    set status enable >> Send logs to syslog
    set server "10.200.20.20" >> FortiNAC eth0 IP address
    set source-ip "10.200.20.1". >> FortiGate IP address in FortiNAC Topology View
    set format csv
end

config log syslogd filter
    set filter "logid(0101039947,0101039948,0101037129,0101037134)" >> syslog ids
end

config log eventfilter
    set event enable >> Enable event logging
    set vpn enable >> Enable VPN activity event
end
```

FortiOS 7.0 and above

```
config log syslogd setting
    set status enable >> Send logs to syslog
    set server "10.200.20.20" >> FortiNAC eth0 IP address
    set source-ip "10.200.20.1". >> FortiGate IP address in FortiNAC Topology View
    set format csv
end

config log syslogd filter
    config free-style
        edit 1
            set category event >> Event log type
            set filter "(logid 0101039947 0101039948 0101037129 0101037134)"
        next
    end
end

config log eventfilter
    set event enable >> Enable event logging
    set vpn enable >> Enable VPN activity event
end
```

Build VPN tunnel. Proceed to the appropriate section:

[SSL VPN](#)

[IPSec VPN](#)

SSL VPN

Important: When SSL VPN Settings are applied, all existing SSL VPN connections are disconnected, regardless of portal. Applying SSL VPN Settings should be done during a Maintenance Window.

Configure the VPN portals and settings:

- Address Object(s) configured with the VPN scope(s) just created
- Production DNS server IP address for DNS Server #1
- FortiNAC's VPN interface address for DNS Server #2
- Domain Name for agent communication (required if agents are delivered through Captive Portal):
 - Must match the domain to be configured in the VPN scope of FortiNAC. FortiNAC only answers SRV queries from connecting agents sourced from this domain. See [DNS File Entry Descriptions](#) in the Appendix for details.
 - If FortiNAC is managing multiple VPN scopes where agents are delivered through the portal, they must all use the same domain.
 - Avoid using .local suffix. macOS and some Linux systems may have communication issues.

VPN Portals

UI

1. Navigate to **VPN > SSL-VPN Portals**
2. Configure using VPN IP address objects just configured
3. Click **OK** to save

Dashboard

Security Fabric

FortiView

Network

System

Policy & Objects

Security Profiles

VPN

Overlay Controller VPN

IPsec Tunnels

IPsec Wizard

IPsec Tunnel Template

SSL-VPN Portals

SSL-VPN Settings

VPN Location Map

User & Device

WiFi & Switch Controller

Log & Report

Monitor

Edit SSL-VPN Portal

Name

FNAC_SSL_Portal

Limit Users to One SSL-VPN Connection at a Time

Tunnel Mode

Enable Split Tunneling

Source IP Pools

FNAC_SSL_VPN_ADDR

+

Tunnel Mode Client Options

Allow client to save password

Allow client to connect automatically

Allow client to keep connections alive

DNS Split Tunneling

Host Check

Enable Web Mode

Portal Message

SSL-VPN Portal

Theme

Blue

Show Session Information

Show Connection Launcher

Show Login History

User Bookmarks

Predefined Bookmarks

+ Create New

Edit

Delete

Search

Q

Name	Type	Location	Description
No results			

Enable FortiClient Download

Download Method

Direct

SSL-VPN Proxy

Customize Download Location

OK

Cancel

CLI Example

```

config vpn ssl web portal
  edit "FNAC_SSL_Portal"
    set tunnel-mode enable
    set web-mode enable
    set ip-pools "FNAC_SSL_VPN_ADDR"  >> Address Object
    set split-tunneling disable
    set dns-server1 10.200.20.50      >> Production DNS
    set dns-server2 10.200.5.22      >> FortiNAC ETH1_VPN Interface IP
    set dns-suffix "Internal-Lab.info" >> Set Domain Name as DNS-Suffix
  config bookmark-group
    edit "gui-bookmarks"
    next
  end
next
end

```

VPN Settings

Important:

- Applying SSL VPN Settings disconnects all existing SSL VPN connections on the FortiGate. If there are VPN tunnels in production, this should be done during a Maintenance Window.
- VPN settings should be configured via CLI in order to apply them to the specific portal (UI configures *all* SSL portals).
- Domain Name for agent communication

config vpn ssl settings

```
set ssl-min-proto-ver tls1-1
set servercert "Fortinet_Factory"
set tunnel-ip-pools "FNAC_SSL_VPN_ADDR"
set dns-suffix "Internal-Lab.info"    >> Set Domain Name as DNS-Suffix
set dns-server1 10.200.20.50    >> Production DNS
set dns-server2 10.200.5.22    >> FortiNAC ETH1_VPN Interface IP
set port 4443
set source-interface "wan1"
set source-address "all"
set source-address6 "all"
set default-portal "full-access"
config authentication-rule
    edit 2
        set groups "SSL-Users"
        set portal "full-access"
    next
    edit 3
        set groups "FortiNAC RADIUS"    >> RADIUS server user group
        set portal "FNAC_SSL_Portal"    >> Apply to "FNAC_SSL_Portal" only
    next
end
end
```

Proceed to [Configure FortiNAC](#).

IPSec VPN

UI: VPN > IPsec Wizard

For instructions, refer to the following document (Tip: Open in New Tab):

<https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/786021/configuring-the-ipsec-vpn>

- Use the VPN IP address objects previously configured
- Enter your production DNS server IP address for ipv4-dns-server1
- Add the FortiNAC RADIUS server User Group as the XAUTH User Group.

Note: CLI access may be required for additional tunnel customization as desired.

Edit VPN Tunnel

Tunnel Template

Dialup - FortiClient (Windows, Mac OS, Android)

Convert To Custom Tunnel

Name

IPsec VPN

VPN: IPsec VPN

Comments

Network

IP VersionIPv4

Incoming Interface

wan1

Use system DNS in mode config☐

Assign IP From

☒ Address/Address Group

IPv4 mode config

☒

Client Address Range

FNAC_IPsec_VPN_ADDR

Subnet Mask255.255.255.0

DNS Server10.200.20.50

Enable IPv4 Split Tunnel☒

Accessible Networks

IPsec VPN_split

Forward Error Correction

Egress ☐ Ingress ☐

Authentication

Authentication Method : Pre-shared Key

XAUTH

User Group: FortiNAC RADIUS

Login to the FortiGate CLI to complete configuration.

CLI:

Ensure the following is configured on the IP/Sec phase1 interface.

- DNS server IP's (primary= production server, secondary = FortiNAC VPN interface)
- Domain Name for agent communication. This must match the domain configured in the VPN scope in FortiNAC. In order for the FortiNAC agent installed on the remote endpoint to be able to locate the FortiNAC to talk to, the FortiGate must be configured with the domain used by the agent to look up FortiNAC. **NOTE:** If FortiNAC is managing multiple VPN scopes, they must all use the same domain.
- IP range to be managed by FortiNAC

NOTE: DHCP relay is not supported

See commands (in bold) below.

IPsec CLI Example:

```
config vpn ipsec phase1-interface
  edit "IPsec VPN"
    set type dynamic
    set interface "wan1"
    set mode aggressive
    set peertype any
    set net-device disable
    set mode-cfg enable >> In custom mode this is disabled by default
    set ipv4-dns-server1 10.200.20.50 >> Production DNS
    set ipv4-dns-server2 10.200.5.22 >> FortiNAC ETH1_VPN Interface IP
    set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
    set dpd on-idle
    set comments "VPN: IPsec VPN"
    set wizard-type dialup-forticlient
    set xauthtype auto
    set authusrgrp "FortiNAC RADIUS"
    set assign-ip-from name >> Use IP range based on Address Object name
    set ipv4-netmask 255.255.255.0
    set ipv4-split-include "IPsec VPN_split"
    set ipv4-name "FNAC_IPsec_VPN_ADDR" >> Address Object name
    set domain "Internal-Lab.info" >> Set Domain Name as DNS-Suffix
    set save-password enable
    set psksecret ENC
ZsrbpXU3R3L9pTcwh061KMX+GSX4tcwgBovwbHjBZbWKOSiR0K8k4oUUJiXDiXoTOQ7gnKShHkdO
2xGKVQi30rjBP070R9WwBbTU5E+JspO7yneNDeNX5wRNRucP02xkPaHulWBa07LeK47UixWtKN2M
xzPultjy06HXl291U7zyMx1Svzz4K5KTqlXhdkXtKIj4Nw==
    set dpd-retryinterval 60
  next
end
```

Proceed to [Configure FortiNAC](#).

Configure FortiNAC

The following items must be configured on the FortiNAC appliance:

- VPN Isolation interface (including DHCP scopes and domain name)
- Policy Based Routes
- RADIUS/LDAP Authentication
- FortiGate model creation/discovery
- FortiGate model configuration (RADIUS and back-end authentication)
- FSSO settings
- VPN Endpoint compliance policies
- VPN Network Access Configuration policies
- VPN logical network to tag/group mappings
- VPN Captive Portal Content

Isolation Interfaces

Configure the eth1 VPN isolation interface using Configuration Wizard.

1. Launch the Configuration Wizard by opening a browser and navigating to:
`https://<FortiNAC IP Address or hostname>:8443/configWizard`
2. Enter the Configuration Wizard credentials.

User Name = config

Password = <configWizard password>
3. Click **OK** at the License Key prompt.
4. Click **OK** at the Download Documentation page.
5. On the left, click **Virtual Private Network**.
6. Click the checkbox for **Virtual Private Network Interface eth1**.
7. Configure the eth1 interface using the table below.

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 (optional)	IPv6 address for the VPN interface on eth1.
Interface IPv6 Mask in CIDR notation (optional)	Subnet IPv6 mask for the VLAN interface in CIDR notation format (e.g., 64).
Interface IPv6 Gateway(optional)	IPv6 Gateway for the VLAN interface for eth1 when clients connect through this VLAN.

8. Under **Virtual Private Network Scopes**, click **Add**.

9. Configure using the table below.

Label	Desired name for VPN DHCP scope Note: When setting up Layer 3 Network Configurations in the Configuration Wizard, labels of DHCP Scopes should not begin with any of these strings: "REG_", "REM_", "AUTH_", "DE_", "ISOL_", "VPN_", or "HUB_". These are reserved.
Gateway	Default gateway for the client lease pool you are adding. Do not use the default gateway for eth1.
Domain	Must match the domain value configured in the FortiGate. NOTE: <ul style="list-style-type: none">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.
Mask	Subnet mask for the default gateway.

10. Under **Lease Pools** click **Add**.

11. Enter the IP Addresses for **Start** and **End** of the lease pool range for the VPN scope defined in the FortiGate Address Object.

12. Click **Add** to save.

13. Click **Apply**.

14. Repeat steps 10 – 13 for additional VPN scopes as needed

15. Click **Summary** when finished.
16. Review the data on the Summary View to confirm the configured settings.
17. Click **Apply**. The Configuration Wizard writes the data to the files on the appliances. This process may take several minutes to complete. When completed, the Results page appears.
18. Review the Results. Errors are noted at the top of the Results page.
19. Scroll down through the results and note errors or warnings. Make changes and apply them until a successful configuration is written.

Example values:

FortiNAC CA FQDN: Server01.Fortinet.com

Eth0 (Management interface): 10.200.20.20

Registration interface: 10.200.5.20

Remediation interface: 10.200.5.21

VPN interface: 10.200.5.22

Eth1 GW: 10.200.5.1

VPN DHCP range (SSL): 10.200.80.10- 10.200.80.99

VPN DHCP range (IPSec): 10.200.80.100 – 10.200.80.200

20. After committing the changes in Configuration Wizard, run the command `ifconfig` in the FortiNAC 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 10.200.20.20 netmask 255.255.255.0 broadcast 10.200.20.255

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 10.200.5.20 netmask 255.255.255.0 broadcast 10.200.5.255
      inet6 fe80::20c:29ff:fe71:e423 prefixlen 64 scopeid 0x20<link>
      ether 00:0c:29:71:e4:23 txqueuelen 1000 (Ethernet)

eth1:1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 10.200.5.21 netmask 255.255.255.0 broadcast 10.200.5.255

eth1:2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 10.200.5.22 netmask 255.255.255.0 broadcast 10.200.5.255 << VPN
```

Proceed to [Policy Based Routes](#).

Policy Based Routes

Configure policy-based routing. Policy-based routing ensures traffic is transmitted out the same interface it was received. This allows FortiNAC agents to communicate to FortiNAC through both the management (eth0) or VPN sub-interface depending on whether the endpoint is isolated or not.

Policy-based routing is configured on FortiNAC using the command: **setupAdvancedRoute** which is run from a FortiNAC 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.

Important: If High Availability is configured, execute the steps outlined in sections **Isolation Interfaces** and **Policy Based Routes** on the Secondary Server and make the same modifications. Otherwise, VPN will not work should a failover occur.

1. Login to the CLI as root of the FortiNAC server (Application Server if separate Control and Application Servers)
2. 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.
3. 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
```

4. Reboot appliance.

System Defined Uplink Count

Ensure the System Defined Uplink Count value is larger than the maximum number of VPN clients that could be online at the same time. Otherwise, the VPN virtual port in FortiNAC could be changed to an uplink. All clients would then be marked as offline and the FSSO tags removed, affecting network access. For details on setting this value, see **System Defined Uplink Count** in section [Network device](#) of the Administration Guide.

Authentication Server Settings

To authenticate VPN network users, FortiNAC must have either a RADIUS server or a LDAP directory configured. If the desired authentication server is not already configured in FortiNAC, refer to the following sections in the Administration Guide for instructions (Tip: Right Click on the link and select **Open in New Tab**):

- [Configure RADIUS settings](#)
- [Directory configuration](#)
- [Portal configuration – Configure authentication credentials](#)

Add Device Model

1. In the FortiNAC Administration UI, navigate to **Network Device > Topology**.
2. Discover or add the FortiGate using an IP address owned by the Management VDOM. Include the following:

SNMP Settings: SNMP v1 or v3 credentials used for device discovery and ARP collection/L3 polling


CLI Settings: Administrator account credentials used for API access.

Instructions in the Administration Guide (Tip: Open in New Tab)

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.

The FortiGate will display in Topology as a wireless device  since it can act as a wireless controller. Device Type will show the part number.

Customer

Directories

AD Pingable

AD-2 Pingable

FortiLand

FG81EPTK18005296

FWF60ETK18001947

PU421E3X16005547

PU421E3X16005681

S108EN4N17001579

Switches

Wireless APs

Ports

SSIDs

Element

System

Polling

Credentials

Virtualized Devices

Filter

Add Filter:

Select


Update

Ports - Displayed: 30 Total: 30

<< first < prev 1 next > last >>

300

Status	Device	Label	Name
	FG81EPTK18005296	port9	S108EN4N17001579:port9
	FG81EPTK18005296	port8	S108EN4N17001579:port8
	FG81EPTK18005296	port7	S108EN4N17001579:port7

Since the FortiGate displays as a wireless device, the Network Device Summary panel under **Bookmarks > Dashboard** lists FortiGate models as Wireless Access Points. Clicking on the  icon lists the devices.

Network Device Summary:			
Refresh: Manual			
Device	Total	Operating	Error
Server	2	2	0
Switch	3	3	0
Wireless Access Point	4	4	0
Ports	59	56	3

Network Device Summary - Wireless Access Point (Online)	
Wireless Access Point (Online) - Total: 4	
<< first < prev 1 next > last >> 200	
Device Name	Description
FG81EPTK18005296	
FWF60ETK18001947	FortiWifi 60E
PU421E3X16005547	PU421E3X16005547
PU421E3X16005681	PU421E3X16005681

- Once added, right click on the model and select **Resync Interfaces**. The ports will be listed under the **Ports** tab.
- Enable L3 Polling. Right click on the model in the left panel and select **Group Membership**.
- Check the box next to **L3 Polling (IP→MAC)** and click **OK**.
- Click the **Polling** tab.
 - Check the box next to **L2 Hosts Polling**. If configuring Device Detection traps, set the **L2 (Hosts) Polling** value for 15 minutes.
 - Check the box next to **L3 (IP→MAC) Polling**.
 - Click **Save**.

Once the FortiGate is discovered, new VPN interfaces in the Ports view will appear. The new interface is created for the FortiGate device model with the name format:

<VDOM name>_<IPSEC_VPN or SSL_VPN>

Branch 1

FGT-Branch-01

PU421E3X16005681:FAP-E

Branch 2

Corporate Engineering

Corporate IT

Corporate User

Self Config

Filter

Add Filter:

Select

Update

Ports - Displayed: 14 Total: 14

<< first < prev 1 next > last >>

300

Status	Device	Label	Name	IP Address	Connection State	Default VLAN	Current VLAN	Admin Status
<input checked="" type="checkbox"/>	FGT-Branch-01	root_IPSEC_VPN	FGT-Branch-01 VPN root_IPSEC_VPN		Not Connected			Off

<input checked="" type="checkbox"/>	FGT-Branch-01	root_SSL_VPN	FGT-Branch-01 VPN root_SSL_VPN		Not Connected			Off
-------------------------------------	---------------	--------------	--------------------------------	--	---------------	--	--	-----

- If utilizing the FortiGate REST API key (FortiNAC versions 8.8.3 and greater), login to the FortiNAC CLI as root and enter the following:

Device -ip <FortiGate model IP> -SetAttr -name APIToken -value <API Key>

FortiGate Device Model Configuration

Must be configured for each VDOM sending RADIUS to FortiNAC (Multiple VDOM/Split-Task VDOM support requires FortiNAC version 8.8.8, 9.1.2 or greater).

- Right-click on the new model and select **Model Configuration**.

General

User Name Password

Protocol

Type SSH 2

RADIUS

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

Authentication Method

☐ RADIUS ☐ LDAP

Apply Reset

- RADIUS:** Enter a value for the RADIUS secret. This must match the one entered on the FortiGate for the RADIUS server definition created for FortiNAC.
- Authentication Method:** Select authentication method to proxy VPN User authentication. Note: If neither method is selected, LDAP is used.

Logical Networks

1. In the Administration UI, navigate to **Network Devices > Topology**.
2. Click the FortiGate device.
3. Under the **Virtualized Devices** tab, right-click the VDOM in which the VPN tunnel is configured and select **Model Configuration**.
4. Define the **Source IP Address**. This is the IP address the FortiGate Fabric Connector will use for communication over the Security Fabric. Required if the VPN tunnel is configured on a VDOM other than the one owning the IP address defined in the **Element** tab.
5. Associate Logical Network(s) to the Firewall Tags or Groups that will be sent to the FortiGate. The Tags/Groups will be imported to the FortiGate once the Security Fabric connection is completed in later steps.

Enter or choose the desired Firewall tag values or group entries to send to the FortiGate when the VPN client is identified.

VPN_AUTHORIZED	<input type="text" value="VPN_AUTH"/>	<input type="checkbox"/>	<input type="button" value="Any Groups"/>
----------------	---------------------------------------	--------------------------	---

For more details, refer to the below section in the Administration Guide (Tip: Open in New Tab):
[Logical networks](#)

Security Fabric Communication

FortiNAC must be configured as a security fabric connector on the FortiGate. Therefore, a few settings need to be configured in FortiNAC to prepare for the FortiGate to connect to it.

1. Navigate to **System > Settings > System Communication > Fortinet FSSO Settings**.
2. Select **Enable FSSO Communication**.
3. Leave the port set to 8000 unless it has been changed on the FortiGate.
4. Enter the password that will be used in the fabric connector definition on the FortiGate.

Fortinet FSSO Settings	
<input checked="" type="checkbox"/> Enable FSSO Communication	
Port:	<input type="text" value="8000"/>
Password:	<input type="password" value="*****"/> <input type="button" value="Show"/>

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 policy, this page will allow them to download the Supplicant Configuration. This is primarily used for Apple iOS devices as other devices will download the supplicant configuration via the Agent. 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 the following section in the Administration Guide (Tip: Open in New Tab): [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 (Tip: Open in New Tab): [Portal Policies](#)

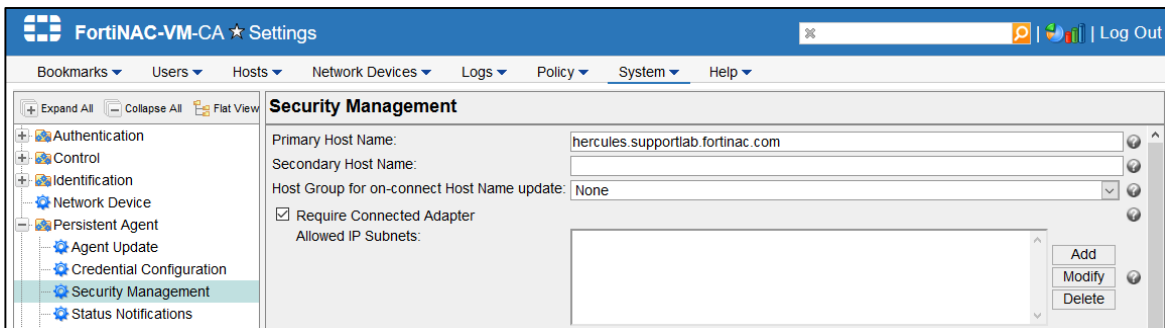
Persistent Agent Configuration

If the Persistent Agent will not be used, skip this step and proceed to Default Endpoint Compliance Policy.

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.



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 IP Pool then click **OK**. This allows FortiNAC to communicate with agents from that network regardless of connection status.

Example:

IP Address: 10.200.80.0

CIDR/mask: 24

For more details, refer to the following section in the Administration Guide (Tip: Open in New Tab): [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 details, refer to the following section in the Administration Guide: For more information on this setting, see section **Persistent Agent Settings** in the Persistent Agent Deployment Guide (Tip: Open in New Tab): [Persistent Agent Deployment and Configuration](#)

To disable the messaging 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

Default Endpoint Compliance Policy (Optional)

Endpoint compliance is a feature set used to ensure hosts connecting to the network comply with network usage requirements. Create a default VPN Endpoint Compliance Policy to:

- Distribute an agent via captive portal for isolated machines that do not have an agent already installed. Note: If endpoints are expected to have an agent already installed prior to connecting, this function may not be required.
- Scan the machine to determine if security requirements are met (Anti-Virus programs, operating system, etc).

If these functions are not required, skip this step and proceed to [Network Access Policies](#).

[Create a Security Scan](#)

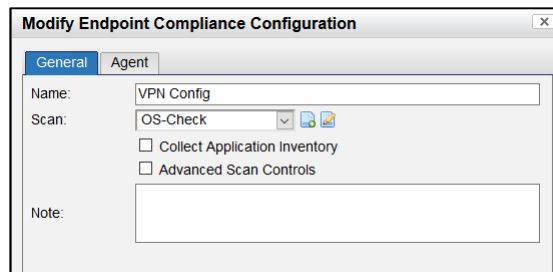
1. Navigate to **Policy > Policy Configuration**.
2. Under **Endpoint Compliance** click **Scans**.
3. Configure the scan to check for required programs and/or files. For more details, refer to the following section in the Administration Guide (Tip: Open in New Tab): [Add or modify a scan](#)

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.

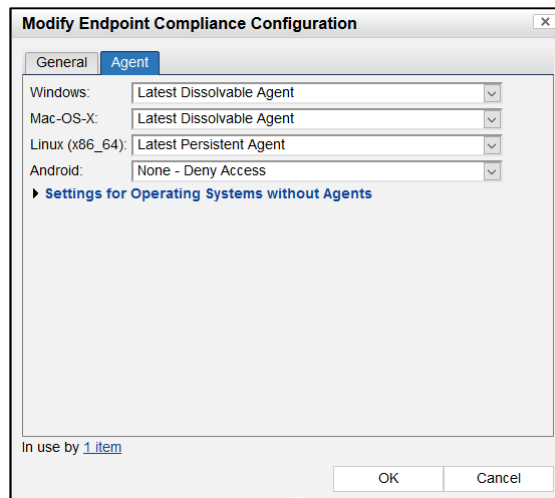
- **Dissolvable Agent (DA):** Downloaded and installed every time the user connects to the network. After scanning the user's PC and reporting results to FortiNAC, the agent removes itself.

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 (Tip: Open in New Tab): [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 (*)>]

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

2. Click **OK**.

For more details, refer to the following section in the Administration Guide (Tip: Open in New Tab): [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 (Tip: Open in New Tab): [Add or Modify a policy](#)

Network Access Policies

Configure Network Access Policies for the IP address ranges used for VPN access. If multiple IP address ranges are used for different types of VPN access (SSL or IPSec), different policies can be created or they can be combined into a single policy.

Configuration Steps

1. Create a **User/Host Profile** with the following for each level of access (such as Staff and Executives):
 - IP scopes that correspond to the addresses used for the VPN types being managed
(Adapter Tab) IP Address: <VPN IP subnets>
 - Other who/what/when information as appropriate
 - Prevent at-risk hosts from connecting to VPN:
Host [Security Status: Safe]
 - Prevent disabled hosts from connecting to VPN:
Host [Access Status: Enabled]
 - Alternatively, create Network Access Policy for just disabled or at-risk where they are sending a different tag for a different ACL.
Host [Security Status: At Risk]
Host [Access Status: Disabled]
2. Choose an existing one for the desired VPN network to assign to VPN sessions.
3. Create a **Network Access Configuration** that references the Logical Network chosen for VPN sessions
4. Create a **Network Access Policy** that uses both the new VPN User/Host Profile and Network Access Configuration
5. Adjust the rank of the Network Access Policy as appropriate

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

Proceed to [Finalize Configuration](#).

Finalize Configuration

Establish Security Fabric Connection with FortiGate

Have both FortiGate and FortiNAC UI's open for the following steps.

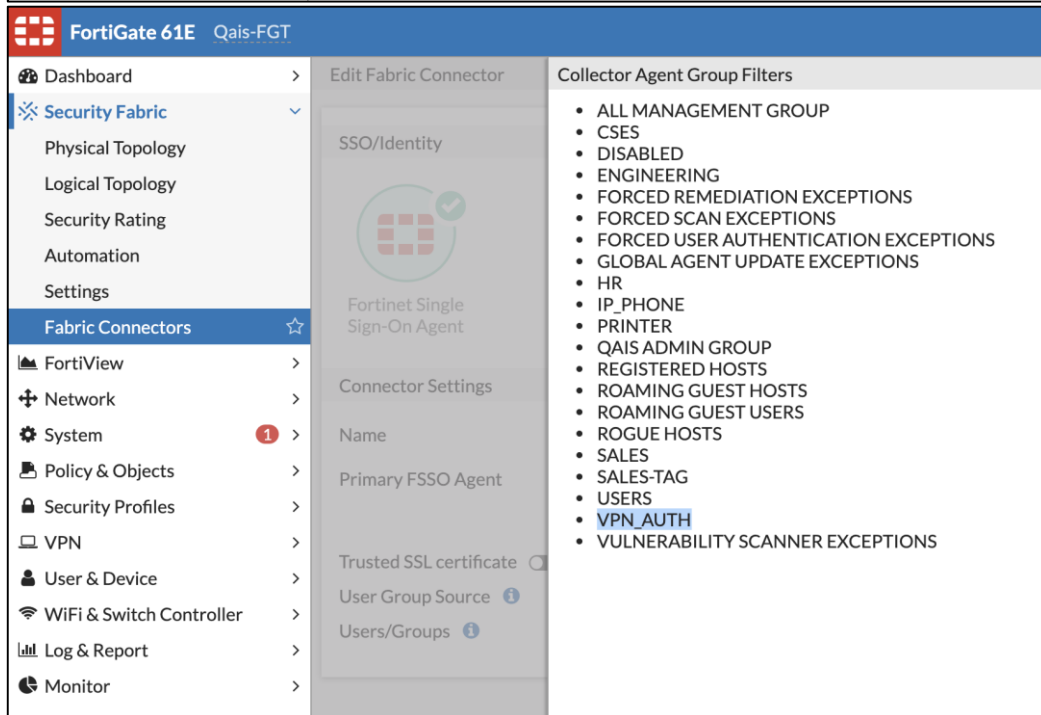
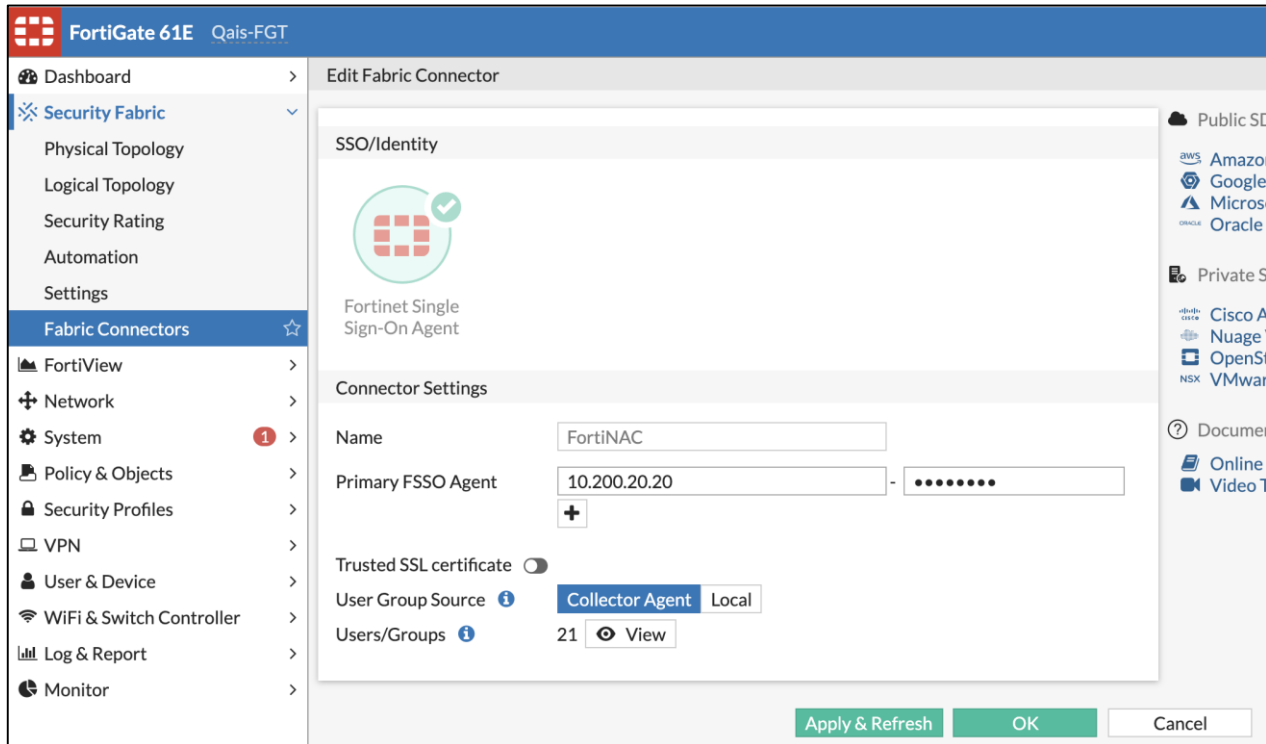
1. In the *FortiGate UI* under the VPN tunnel's VDOM
 - a. Navigate to **Security Fabric > Fabric Connectors**.
 - b. Enter IP address of primary FortiNAC interface (eth0).
 - c. Enter password used in FortiNAC for FSSO settings.
 - d. Click **OK** to save.
 - e. Right click on the new connector and select **Edit**.
 - f. Define the IP address the Fabric Connector will use for communicating with FortiNAC. If VPN is configured within the Management VDOM, enter the address used to model the FortiGate in Topology.

If FortiGate UI does not provide this option, configure via FortiGate CLI.

Commands

```
config user fsso
edit "<FSSO Connector name>"
set source-ip <FortiGate IP Address>
```

2. In the *FortiNAC Administration UI*
 - a. Navigate to **Network Devices > Topology**.
 - b. Click the FortiGate device.
 - c. Under the **Virtualized Devices** tab, right-click the VDOM the VPN tunnel is configured and select **Model Configuration**.
 - d. Define the **Source IP Address**. This must match the source IP entered in the previous step.
 - e. Click **Submit Query** at the bottom of the page.
3. In the *FortiGate UI*
 - a. Edit the Fabric Connector and click **Refresh**.
 - b. The FortiGate will read in all the FortiNAC Tags and user/host groups.
 - c. The FortiNAC Tags and user/host groups are now available for use within FortiGate User groups.



FortiOS versions prior to 6.2: Proceed to [Create User Group in FortiGate](#)
FortiOS versions 6.2 and later: Proceed to [Create FortiGate Firewall Policies](#)

Create User Group in FortiGate (Required for FortiOS versions prior to 6.2)

UI: User & Device > User Groups

Create a User Group for each of the imported FortiNAC groups that pertain to VPN (configured to map to the VPN logical network choice). These groups will be used within the FortiGate firewall policies that grant network access to VPN clients.

Dashboard	>	+ Create New Edit Clone Delete <input type="text" value="Search"/>		
Security Fabric	>			
FortiView	>			
Network	>			
System	>			
Policy & Objects	>			
Security Profiles	>			
VPN	>			
User & Device	✓			
User Definition				
User Groups	☆			
Guest Management				
Device Inventory				

Group Name	Group Type	Members
FNAC-VPN	Fortinet Single Sign-On (FSSO)	FNAC_VPN
FortiNAC Radius UG	Firewall	FortiNAC
Guest-group	Firewall	guest
IPS Group	Fortinet Single Sign-On (FSSO)	IPS_HOST-TAG
IPSecVPN	Firewall	ipsecuser
SSL-Group	Fortinet Single Sign-On (FSSO)	SSL_HOST-TAG
SSLVPN	Firewall	ssluser
SSO_Guest_Users	Fortinet Single Sign-On (FSSO)	

Proceed to [Create FortiGate Firewall Policies](#).

Create FortiGate Firewall Policies

Create firewall policies to:

- Allow network access to VPN clients authenticated by FortiNAC (authorized hosts).
- Restrict network access to all other VPN clients. They are considered untrusted.

Workflow:

1. When a client initially connects to the VPN tunnel, network access is restricted.
2. While restricted, FortiNAC answers all DNS queries. Limited network access is granted. The amount of network access allowed is dependent upon the organization's policies. For example, it may be necessary to allow clients to update antivirus programs. In which case, network access to the internet may be required. FortiNAC would control which domains are resolved to the actual IP address.
3. Once authenticated, clients match a FortiNAC Network Access Policy and a Logical Network is assigned. FortiNAC sends the group or tag associated with the Logical Network to the FortiGate.
4. The matching FortiGate firewall policy applies the appropriate network access.

Note:

- The following examples are for illustration purposes. It is up to the firewall administrator to configure their policies as appropriate to achieve the above goals.
- It is assumed the applicable components required for firewall policies have already been configured (such as network interfaces).

UI: Policy & Objects > IPv4 Policy

Allow Network Access for Authorized Hosts

Create Firewall policy to allow network access for authorized hosts:

- **Block** DNS (at a minimum) or all traffic to/from FortiNAC VPN Interface (Ensures DNS requests are forwarded to production DNS).

Block DNS to FortiNAC

Name	Name of Policy
Incoming Interface (From)	Any
Outgoing Interface (To)	FortiNAC VPN Isolation Network
Source	VPN IP Address Object(s) FSSO Group
Destination	VPN Isolation Interface Address
Schedule	Always
Service	DNS or ALL
Action	DENY
Enable this policy	enable

- **Allow** traffic to/from the desired network destinations.

Example

Legend:

FNAC_SSL_VPN_ADDR	VPN IP Address Object (SSL)
FNAC_IPsec_VPN_ADDR	VPN IP Address Object (IPsec)
VPN_AUTH	FSSO Group sent by FortiNAC
SERVER NET	FortiNAC VPN Isolation Network
FNAC_ETH1_VPN	VPN Isolation Interface Address
wan1	Interface to internet
MGMT NET	Internal

ID 10: Block VPN traffic from any network to FortiNAC VPN Interface

ID 11: Allow VPN traffic from any interface out to the internet

ID 13: Allow VPN traffic from any interface to the Management network

+ Create New Edit Delete Policy Lookup <input type="text" value="Search"/> Interface Pair View By Sequence								
ID	Name	From	To	Source	Destination	Schedule	Service	Action
10	VPN AUTH ISOLATION DENY	<input type="checkbox"/> any	SERVER NET.	FNAC_SSL_VPN_ADDR FNAC_IPsec_VPN_ADDR VPN_AUTH	FNAC_ETH1_VPN	always	ALL	DENY
11	VPN AUTH INTERNET ACCEPT	<input type="checkbox"/> any	wan1	FNAC_SSL_VPN_ADDR FNAC_IPsec_VPN_ADDR VPN_AUTH	all	always	ALL	ACCEPT
13	VPN AUTH MGMT ACCEPT	<input type="checkbox"/> any	MGMT NET	FNAC_SSL_VPN_ADDR FNAC_IPsec_VPN_ADDR VPN_AUTH	all	always	ALL	ACCEPT

Restrict Network Access for Unauthorized Hosts

Create policies for managed VPN connections to restrict network access for unauthorized hosts. These are the default policies used until a host is authenticated with FortiNAC.

- **Allow** traffic to/from FortiNAC VPN Interface (to ensure DNS requests are forwarded to FortiNAC)

Name	Name of policy
Incoming Interface (From)	VPN Interface
Outgoing Interface (To)	FortiNAC VPN Isolation Network (Inside)
Source	SSL_VPN Address Object & FortiNAC RADIUS User group
Destination	FortiNAC VPN Isolation Interface address
Schedule	Always
Service	All
Action	ACCEPT

- **Block** all other traffic.

Example

Legend:

FNAC_SSL_VPN_ADDR	VPN IP Address Object (SSL)
FNAC_IPsec_VPN_ADDR	VPN IP Address Object (IPsec)
VPN_AUTH	FSSO Group sent by FortiNAC
SERVER NET	FortiNAC VPN Isolation Network
FNAC_ETH1_VPN	VPN Isolation Interface Address
wan1	Interface to internet
MGMT NET	Internal

ID 9 & 15: Allow SSL and IPsec VPN traffic to the FortiNAC VPN eth1 interface

ID 12 & 16: Block SSL and IPsec VPN traffic to all interfaces

9	SSL_VPN PRE-AUTH ISOLATION ACCEPT	SSL-VPN tunnel interface	SERVER NET.	FNAC_SSL_VPN_ADDR FortiNAC RADIUS	FNAC_ETH1_VPN	✓ ACCEPT
12	SSL_VPN PRE-AUTH DENY ANY	SSL-VPN tunnel interface	MGMT NET wan1	FNAC_SSL_VPN_ADDR FortiNAC RADIUS	all	✗ DENY
15	IPsec_VPN PRE-AUTH ISOLATION ACCEPT	IPsec VPN	SERVER NET.	FNAC_IPsec_VPN_ADDR	FNAC_VPN INTER.	✓ ACCEPT
16	IPsec_VPN PRE-AUTH DENY ANY	IPsec VPN	MGMT NET wan1	FNAC_IPsec_VPN_ADDR	all	✗ DENY

Rank new policies in the following order:

1. Policies matching authenticated users (allowing regular network access)
2. Policies allowing traffic to FortiNAC eth1 (restricting network traffic).

If endpoint does not match a policy that permits regular network access (ID's 10, 11, 13), then endpoint is considered untrusted. Therefore, apply policies to restrict endpoint's network access to the FortiNAC Service Network (ID's 9, 12, 15 16).

Dashboard	+	Create New	Edit	Delete	Policy Lookup	Search	Interface Pair View	By Sequence
Security Fabric								
FortiView								
Network								
System								
Policy & Objects								
IPv4 Policy								
Authentication Rules								
Local In Policy								
IPv4 DoS Policy								
Addresses								
Internet Service Database								
Services								
Schedules								
Virtual IPs								
IP Pools								
Protocol Options								

ID	Name	From	To	Source	Destination	Action
10	VPN AUTH ISOLATION DENY	any	SERVER NET.	FNAC_SSL_VPN_ADDR FNAC_IPsec_VPN_ADDR VPN_AUTH	FNAC_ETH1_VPN	✗ DENY
11	VPN AUTH INTERNET ACCEPT	any	wan1	FNAC_SSL_VPN_ADDR FNAC_IPsec_VPN_ADDR VPN_AUTH	all	✓ ACCEPT
13	VPN AUTH MGMT ACCEPT	any	MGMT NET	FNAC_SSL_VPN_ADDR FNAC_IPsec_VPN_ADDR VPN_AUTH	all	✓ ACCEPT
9	SSL_VPN PRE-AUTH ISOLATION ACCEPT	SSL-VPN tunnel interface	SERVER NET.	FNAC_SSL_VPN_ADDR FortiNAC RADIUS	FNAC_ETH1_VPN	✓ ACCEPT
12	SSL_VPN PRE-AUTH DENY ANY	SSL-VPN tunnel interface	MGMT NET wan1	FNAC_SSL_VPN_ADDR FortiNAC RADIUS	all	✗ DENY
15	IPsec_VPN PRE-AUTH ISOLATION ACCEPT	IPsec VPN	SERVER NET.	FNAC_IPsec_VPN_ADDR	FNAC_VPN INTER.	✓ ACCEPT
16	IPsec_VPN PRE-AUTH DENY ANY	IPsec VPN	MGMT NET wan1	FNAC_IPsec_VPN_ADDR	all	✗ DENY

Enable VPN Management for Existing FortiGate Models

Note: If the FortiGate was modeled during the **Configure FortiNAC** section of this document, this step is not needed. Proceed to [Validate](#).

The VPNManagedNetworks attribute is used to indicate whether VPN tunnel(s) should be managed by FortiNAC for a specific modeled device. The attribute is set on the FortiGate device model in the FortiNAC database.

Perform the following steps if the FortiGate was already modeled in Topology prior to the VPN integration:

1. In the FortiNAC Administration UI, navigate to **Network Devices > Topology**.
2. Select the FortiGate device model in the tree.
3. Right click and select **Network Access/VLANs**.
4. Click **Read VLANs**.

FortiNAC reviews the list of DNS Servers in the FortiGate's VPN configuration. If one of the DNS server IP's match one of the FortiNAC interface IP's, the VPN tunnel is considered to be managed. FortiNAC updates the FortiGate device model's VPNManagedNetworks attribute value.

This can be confirmed in the FortiNAC CLI using the command:

device -ip <FortiGate IP>

Look for the attribute name **VPNManagedNetworks**.

Example:

Name = VPNManagedNetworks value = FNAC_SSL_VPN_ADDR << FortiGate address
Object Name used by VPN tunnel

Proceed to [Validate](#).

Validate

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

1. Host is assigned an IP address from the VPN address pools defined on the FortiGate and in Configuration Wizard.
2. If an agent is not already installed on the connecting host, depending on the VPN Endpoint Compliance Policy, the user may be prompted to download an agent. Without an agent, the VPN session will not be authorized by FortiNAC.
3. If agent is installed, the appropriate scan configured in the VPN Endpoint Compliance Policy is run.
4. Once the scan completes and passes, FortiNAC sends the FSSO tag/group values to the FortiGate which changes the firewall rules that match the VPN traffic from that point forward, and the host is granted access to the appropriate networks.

For unexpected behavior, see [Troubleshooting](#).

Troubleshooting

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

1. Proper route(s) are defined to send traffic to FortiNAC from the VPN device. This may include running the **setupAdvancedRoute** tool to create policy-based routes.
2. The remote IP assigned to the VPN session comes from the correct VPN pool on the FortiGate and the address scope is correctly defined for the VPN context on the FortiNAC appliance.
3. SNMP and CLI credentials are configured correctly on both FortiNAC and the VPN device to facilitate device discovery and FortiNAC/FortiGate communication.
4. The RADIUS secret is the same on the VPN device, the FortiNAC RADIUS server configuration and the FortiNAC model configuration for the VPN device. Ensure FortiNAC is authenticating the VPN sessions as they connect.
5. The FortiNAC Server or Control Server should always be able to communicate with the FortiGate via FSSO to set and remove tags/groups as appropriate.
6. Firewall policies and routes are defined to allow users on both restricted and non-restricted networks to access the FortiNAC VPN interface.
7. Endpoint compliance and Network access control policies are configured correctly on the FortiGate to match the VPN sessions being managed.
8. Logical Network to tag/group mappings are configured correctly on the FortiGate model in FortiNAC to cause the correct values to be sent to the FortiGate when the session is authorized.
9. Syslog messages are configured to be sent to FortiNAC. Log messages with ids of 0101039947 and 0101039948 (SSL), or 0101037129 and 0101037134 (IPSec) must be sent to FortiNAC.

Related KB Articles

[Troubleshooting FortiGate VPN integrations](#)

[Unable to model FortiGate in High Availability mode](#)

[RADIUS timeout during 2 Factor Authentication](#)

Debugging

RADIUS activity:

```
CampusMgrDebug -name RadiusManager true
```

Syslog activity:

```
CampusMgrDebug -name SyslogServer true
```

FortiGate VPN specific:

```
CampusMgrDebug -name FortinetVPN true
```

VPN activity

```
CampusMgrDebug -name RemoteAccess true
```

Persistent Agent activity:

```
CampusMgrDebug -name PersistentAgent true
```

Dissolvable Agent activity:

```
CampusMgrDebug -name AgentServer true
```

Disable debugging:

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

FortiNAC Network association to each FortiGate:

```
CampusMgrDebug -name DeviceInterface true
```

SSO activity:

```
CampusMgrDebug -name SSOManager true
```

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

Appendix

VPN Connection Process Details

The following sequence describes the process for remote users that connect to the network through a FortiGate VPN when network access is controlled by FortiNAC.

1. A user starts their VPN client.
2. The user enters their user credentials required by the FortiClient or other VPN client. A connection request is sent to the FortiGate VPN device.
3. The FortiGate VPN device sends a RADIUS authentication request to FortiNAC containing the user credentials of the connecting client and requests authentication.
4. FortiNAC proxies the request to either a terminating RADIUS server or LDAP Server.
5. If the user is authenticated, FortiNAC returns an access accept response to the FortiGate VPN device and the user is allowed on the network.
6. When the user is authenticated, the FortiGate VPN device assigns the VPN connection an IP address, production and FortiNAC VPN DNS addresses, and DNS suffix information.
7. The default VPN firewall policies impose restrictions on the user's network access. The rules restrict the user's IP address from reaching anything other than FortiNAC and those sites designated by FortiNAC, such as for certificate validation or remediation.
8. The FortiGate VPN device sends FortiNAC a syslog message when the remote session is established.
9. FortiNAC parses the user and remote IP address of the new session from the syslog message.
10. All VPN Session DNS queries are redirected to the FortiNAC VPN captive portal, since the firewall policies are blocking access to production DNS. The user must already have or download and run an agent. The administrator can provide either the Persistent Agent or the Dissolvable Agent.
11. Once the user has run an agent, the agent locates and identifies an FortiNAC system to connect with using the DNS suffix information provided by the VPN client.
12. The agent obtains a scan policy from FortiNAC based on matching the VPN user/host profile and scans the user's machine. The agent then sends FortiNAC the machine information, including the MAC addresses of all its interfaces and the results of the scan.
13. Once FortiNAC has learned about the machine from the agent, it locates or creates a host to represent it and connects the host to the appropriate VPN interface on the FortiNAC model.
14. If the user's machine fails the scan, the host is marked at risk and 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 their machine. The user should disconnect from the VPN device and make corrections before reconnecting.
15. If the PC is not known to FortiNAC, it is registered either as a machine or to the authenticated user.
16. Once the machine is identified and connected in FortiNAC, it sends the FortiGate FSSO tag/group information appropriate to the FortiNAC Network Access configuration policy

and FortiGate logical network mappings. These tags/groups modify which firewall rules are applied to the session according to how the firewall policies on the FortiGate are configured.

SSL VPN Settings (UI)

Important:

- Applies SSL settings to all portals.
- When SSL VPN Settings are applied, all existing SSL VPN connections are disconnected. Applying settings should be done during a Maintenance Window.

4. Navigate to **VPN > SSL-VPN Settings**

- Enter production DNS server IP address for DNS Server #1
- Enter FortiNAC's VPN interface address for DNS Server #2
- Create an Authentication/Portal Mapping containing the FortiNAC RADIUS server User Group just created. Click **Apply** to save

SSL-VPN Settings

Connection Settings ⓘ

Listen on Interface(s) wan1 + ×

Listen on Port 4443

Web mode access will be listening at <https://94.203.255.199:4443>

Redirect HTTP to SSL-VPN ☐

Restrict Access Allow access from any host Limit access to specific hosts

Idle Logout ☒

Inactive For 300 Seconds

Server Certificate Fortinet_Factory

You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). It is recommended to purchase a certificate for your domain and upload it for use. [Click here to learn more](#)

Require Client Certificate ☐

Tunnel Mode Client Settings ⓘ

Address Range

Automatically assign addressesSpecify custom IP ranges

IP Ranges

FNAC_SSL_VPN_ADDR

+

×

DNS Server

Same as client system DNSSpecify

DNS Server #1

10.200.20.50

DNS Server #2

10.200.5.22

Specify WINS Servers

☐

Authentication/Portal Mapping ⓘ

+ Create New

Edit

Delete

Users/Groups ⌵	Portal ⌵
All Other Users/Groups	full-access
<div>FortiNAC RADIUS</div>	FNAC_SSL_Portal
<div>SSL-Users</div>	full-access

Apply

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. This file is modified when the eth1 VPN isolation interface is configured/modified using Configuration Wizard. 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 **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, FortiNAC 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**, FortiNAC 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 FortiNAC 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 FortiNAC 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 FortiNAC 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, FortiNAC first looks for a route containing the source IP's network in the individual table. If no route for that network is found, FortiNAC 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
7. Proceed to Authentication Server Settings.

Disable Persistent Agent Notifications

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

All agent notifications when connecting over VPN

Disable: `device -ip <FortiGate_IP> -setAttr -name DisableClientTransitionMessages -value true`

Re-enable: `device -ip <FortiGate_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 <FortiGate_IP> -setAttr -name DisableRestrictMessageText -value true`

Re-enable: `device -ip <FortiGate_IP> -setAttr -name DisableRestrictMessageText -value false`

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

Disable: `device -ip <FortiGate_IP> -setAttr -name DisableClearMessageText -value true`

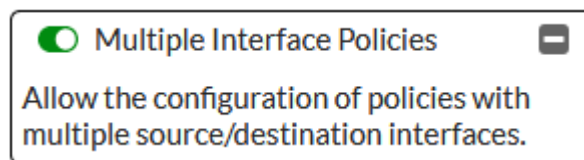
Re-enable: `device -ip <FortiGate_IP> -setAttr -name DisableClearMessageText -value false`

Proceed to [Default Endpoint Compliance Policy](#)

FSSO Groups on the SSL Interface (6.0.x Only)

1. Enable “Multiple Interface Policies” features under **System->Feature Visibility**

This allows an interface option called “all”
















2. Create a new IP Address Range, using the SSLVPN range

Note: There is a range there by default but its tied to the SSLVPN Interface and can't be used with interface “all”

3. Create a new firewall Policy using:

- a. Incoming Interface “**any**”
- b. Outgoing interface to FortiNAC Eth1
- c. Source is new SSLVPN IP Range and FortiNAC FSSO Group for Rogues
- d. Destination could be refined to just FortiNAC Eth1 interface
- e. Service could be refined to DNS, HTTPS, DHCP, Agent (4567/4568)

Name 	SSLVPN-Init		
Incoming Interface	<input type="checkbox"/> any		
	+		
Outgoing Interface	 Eth1 (port2)		
	+		
Source	 SSLVPN-Range		
	 FNAC-VPN-Rogue		
	+		
Destination	 all		
	+		
Schedule	 always		
Service	 ALL		
	+		
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN		
Firewall / Network Options			
NAT	<input type="checkbox"/>		

ARP Data Collection Prioritization

ARP collection can be done via CLI, API and SNMP. If FortiNAC receives ARP data using more than one method, FortiNAC will update tables based upon following precedence:

1. CLI
2. API
3. SNMP

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.