FortiNAC

Security Fabric/SSO Integration

Version: 8.5, 8.6, 8.7, 8.8

Date: March 29, 2022

Rev: Q

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

The information in this document provides guidance to integrate FortiNAC with FortiGate to further enhance FortiGate's Intent-based Segmentation. This integration allows organizations to achieve granular access control, continuous trust assessment, end-to-end visibility and automated threat protection.

What it Does

Single Sign-On (SSO) is the authentication protocol by which users can transparently authenticate to FortiGate. FortiNAC acts as a Collector Agent: It collects and compiles information about user logons. The information is sent to the FortiGate over TCP port 8000 in the form of Logon and Logoff events. These events contain:

- Device Information: IP address
- User information: User ID or MAC address (if no User ID)
- User Group Filter: FortiNAC User Group, Host Group or Firewall Tag

Logon/logoff event information: dynamic, real-time information the FortiGate learns and uses to dynamically match against policies and set up connections internally so the user is known without prompting them to log on again.

Logon event triggers:

- "Registered" device connect
- User logon
- IP change
- Device status change

Logoff event triggers:

- User logoff
- Device disconnect

FortiGate creates one or more log entries for this logon/logoff events as appropriate.

When a user tries to access network resources, the FortiGate unit can use the firewall user list to match a firewall policy with a source group as criterion. If the IP address is known along with the user information and User Group, the policy can be matched.

For more information on SSO, see the FortiOS documentation at docs.fortinet.com.

How it Works

- When an online registered device matches a FortiNAC Network Access Policy, FortiNAC sends to the FortiGate one of the following:
    - Firewall Tag
    - User or Administrator Group
    - Host Group

  Note
  Network Access Policies do not match:
    - Unregistered (Rogue) devices
    - Offline registered hosts

  Therefore, this process would not apply.

- FortiGate regularly polls FortiNAC and imports those Firewall Tags and groups. These can be used to create SSO User Groups. The SSO User Groups are used to build IPv4 policies in order to apply the network access segmentation.
- When a registered device's connection status changes, FortiNAC sends SSO message to FortiGate containing:
    - IP address - Device
    - User ID or MAC address - User
    - Group – Group Filter
        - User Group, Host Group or Firewall Tag defined within FortiNAC
- FortiGate uses this information to build a SSO session and apply the appropriate IPv4 policy to the device.
- As devices disconnect, FortiNAC updates the FortiGate. The SSO session is torn down and the policies previously applied are removed.
- Host status takes precedence over a matching policy. For example, FortiNAC will not apply a matching policy for network access if the registered device is marked At-Risk. Instead, the At-Risk device would be provisioned the "Quarantine" network access as configured in the FortiGate device model.

For a more details, see Connection Process in the Appendix.

Versions 8.8.11, 9.1.5, 9.2.2 and greater: FortiNAC automatically resynchronizes with the FortiGate every 15 minutes. If FortiNAC detects the FortiGate is missing SSO sessions, FortiNAC will re-add them.

FortiGates/FortiSwitches managed by FortiManager: When FortiNAC makes any changes to the FortiGate or FortiSwitch, the Fortigate/FortiSwitch updates FortiManager. This keeps FortiManager in sync.

Requirements

FortiNAC

- Software Engine Version: 8.5 or greater
- Recommended Engine Version: 8.8.5 or greater
- Multiple VDOM/Split-Task VDOM support (includes Split-Task VDOM): Version 8.8.8, 9.1.2 or greater

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. See KB article 193514 for details
- Enable FortiGate admin-https-ssl-versions tlsv1-2. Tlsv1-3 is not supported.
- SNMP community or account
- Administrator account
  - Visibility only: System read access to all VDOMs
  - Control: System read/write access to all VDOMs

- Do no block port 8000 between the FortiNAC and the FortiGate.

Considerations

- FortiNAC will frequently poll the FortiGate for L3 information. For details see Appendix.
- FortiGate can only support one SSO agent sending tags for a specific endpoint IP address. If there are multiple agents, the FortiGate entries will be overwritten when other SSO agents send information for the same endpoint IP. Therefore, the following should be done prior to integration:
  - Identify any other SSO 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:

    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 SSO logon events

    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 SSO agent for the managed endpoint IP address scope.
- Fabric connector connections and firewall policies can be configured at the Fortigate or the FortiManager. For the purposes of this document, a single Fortigate integration is being configured.
- The FortiGate will remove all of the applicable SSO Logins when a Collector Agent (FortiNAC) has been disconnected for 300 seconds (5 minutes). This 5-minute period is internally hard set on the FortiGate and not configurable.

Integration

Configure FortiNAC

Device Model and Configuration

In order to enable SSO communication, the FortiGate and FortiNAC must first be integrated properly. Configure FortiNAC and integrate FortiGate as instructed in the FortiGate Endpoint Management Integration reference manual.

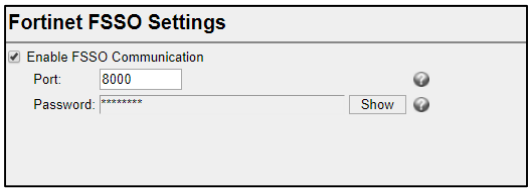
Enable Fortinet SSO Communication

Enable the FortiNAC to communicate with the FortiGate using Fortinet Single Sign-On (FSSO).

1. In the FortiNAC Administration UI, navigate to **System > Settings > System Communication > Fortinet FSSO Settings**
2. Configure using the chart below
3. Click **Save Settings**

FSSO Settings

Enable FSSO Communication	Checked
Port	8000 (Default)
Subnet (8.6.x and lower) **Note: Field removed as of version 8.7**	0.0.0.0/0 (Default)
Password	Must match the password used to configure Fabric Connector in FortiGate (next section)



4. Force SSO Tags to be sent to FortiGate if VLAN is not terminating on FortiGate but some other Layer 3 device. Example: Send tag to FortiGate to apply firewall policy for wireless client connecting to a Cisco WLC.

   Login to FortiNAC CLI as root and type

   device -ip <FortiGate IP address> -setAttr -name ForceSSO -value true

   Caveats:

- The same SSO messaging will be sent to all FortiGates whose models have this function enabled and has selected the matching Logical Network.
- User host profiles should contain criteria to limit the matching hosts to only those desired to have FGT policies applied. SSO messages will be sent for any device matching a network access policy assigning a logical network selected in the FortiGate model configuration.

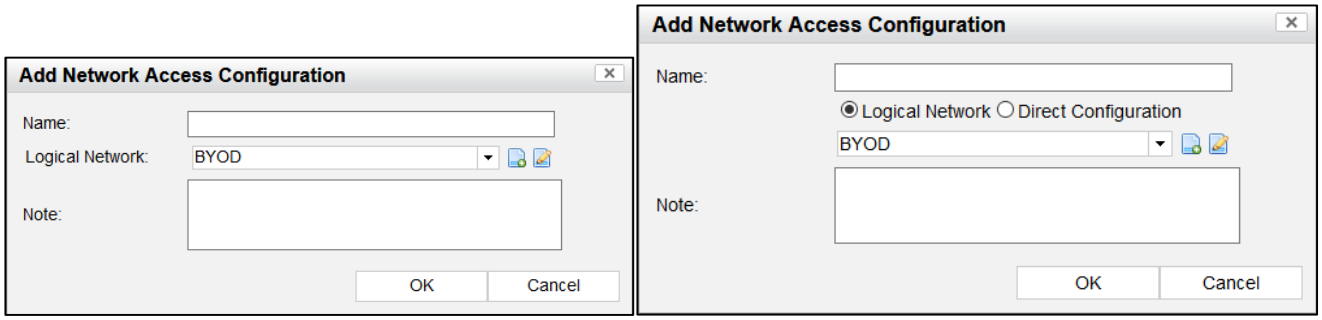
Network Access Policies

Configure policies to provision the appropriate network access when a host connects. For full details on policy configuration, refer to section Network Access Policies of the **Administration Guide** in the Fortinet Document Library.

1. In the FortiNAC Administration UI, navigate to **Policy > Policy Configuration**
2. Create a policy after configuring the following components:
   - **User/Host Profile**: Criteria used to match connecting host
   - **Network Access Configuration**: Specifies the Logical Network or Direct Configuration (in older appliances) to apply when the policy matches.

Assign Logical Network

Select the appropriate logical network from the drill-down menu. If the desired Logical Network is not yet created, click the **Add Logical Network** icon. For details on creating and assigning Logical Networks, see section Logical networks in the Administration Guide.



Direct Configuration (option available in older appliances. Select only if Logical Networks are not used.)

- Specify the appropriate Group or Firewall Tag.
- Create the Firewall (if not yet created)

For details, see Network Access Policy Example (Direct Configuration) in the Appendix.

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 managed 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. Using the table below, define the Source IP (IP address the Fabric Connector will use for communicating with FortiNAC). If FortiGate UI does not provide this option, configure via FortiGate CLI.

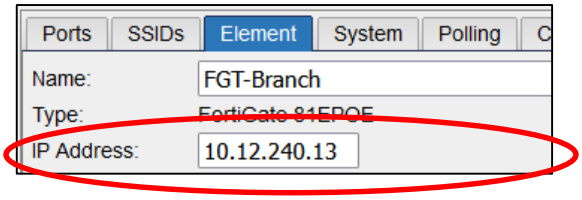
    Commands
    config user fsso
    edit "<FSSO Connector name>"
    set source-ip <FortiGate IP Address>

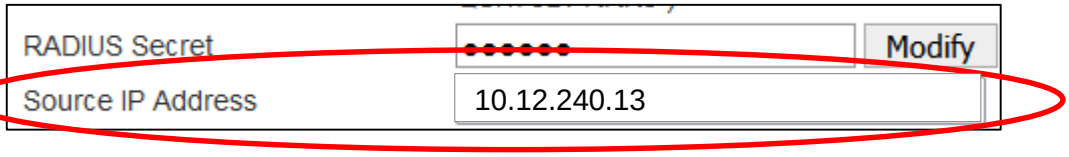
Managed devices are within the Management VDOM	Enter the IP Address used to model the FortiGate in FortiNAC Topology. This can be viewed under the **Element** tab of the device model.
Managed devices are within a non-Management VDOM	Enter the address from which the connector will send SSO messaging. Note this address will also be used in step 2.

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 to be managed and select **Model Configuration.**
    d. Define the **Source IP Address**. **Important:** This value must match the Source IP entered in the previous step (f).
    e. Click **Submit Query** at the bottom of the page.

Example: Managed devices are within the Management VDOM

FortiNAC UI



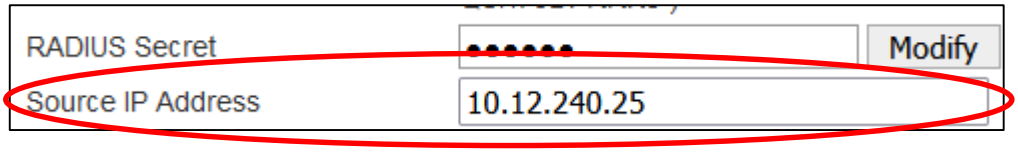


FortiGate CLI

```
config user fsso
edit "FortiNAC Management"
set source-ip 10.12.240.13
```

Example: Managed devices are within a non-Management VDOM

FortiNAC UI



FortiGate CLI

```
config user fsso
edit "FortiNAC Management"
set source-ip 10.12.240.25
```

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
FortiOS versions 6.2 and later: Proceed to Create Firewall Policies

Configure FortiGate

Create User Group (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.

Proceed to Create Firewall Policies.

Create Firewall Policies

In order for proper traffic flow, several policies must be created to manage traffic for the various host states.

1. Navigate to **Policy & Objects > IPv4 Policy**
2. Click **Create New**
3. Configure as appropriate. For examples, see Firewall Policy Examples in the Appendix.
4. Click **OK**

Validate Enforcement

1. Connect a rogue host to one of the managed ports
2. Host receives IP address from FortiGate
3. Upon bringing up browser, the captive portal is displayed (if configured). If portal page is slow to build, certain domains may need to be whitelisted. See KB article Captive Portal Slow to Build.
4. Register the system
5. Once registered, verify the correct Network Access Policy matches in FortiNAC
    a. In FortiNAC UI, navigate to **Hosts > Host View**
    b. Search on host record, right click and select **Policy Details**
6. Verify the correct IPv4 Policy matches in the FortiGate
    a. In FortiGate UI, navigate to **FortiView > Sources**
    b. Double click on host entry
    c. Click **Policies** tab
    d. Hover over policy to verify time last used
7. Confirm user is able to access network resources as expected

If any of the above do not work as expected, refer to the Troubleshooting section of this document.

Troubleshooting

Related KB Articles

Configure and troubleshoot Firewall TAGs
How to list processes in FortiOS (Includes description of each process)
SSO tool script for listing managed networks

Debugging

FortiGate Commands

Enable debugging feature
```
diagnose debug enable
```

Run the applicable debug
":" MAC Address filtering
```
diagnose wireless-controller wlac sta_filter <STA MAC>255 diagnose
```

MAC Authentication / PSK
```
debug application wpad 8 (WPA deamon)
```

802.1X
```
diagnose debug app eap_proxy 31 (EAP deamon)
```

RADIUS Disconnect
```
diag debug app radius-das 8
```

Disable debugging feature
```
diagnose debug disable
```

List currently connected hosts with FSSO sessions:
```
diagnose debug authd fsso list
```

Example output:
```
----FSSO logons----
IP: 172.28.10.2  User: 00:21:70:D1:92:77  Groups: REGISTERED  Workstation:
MemberOf: Registered
Total number of logons listed: 1, filtered: 0
----end of FSSO logons----
```

Enable debug to collect login and FSSO activity (Configure terminal emulation program (Putty, SecureCRT, etc) to save output to a file on the endstation):
```
diag debug reset   << Resets any existing enabled debug to default/off
diag debug console timestamp enable   << Adds timestamps to the debug
diag debug duration 0   << 0 means unlimited. Creates large file over time
diag debug app fcnacd -1   << Device Inventory sessions
diag debug app authd -1    << User sessions
diag debug app fssod -1    << FSSO sessions
diag debug app snmpd -1    << SNMP communication
```

```
diag debug enable   << Starts logging debug to the screen with the prior
configured parameters
```

Disable the debug, then close the session and make sure the output is saved:

```
diag debug disable
diag debug reset
```

FortiNAC Commands

Use the following KB article to gather the appropriate logs using the debugs below.
Gather logs for debugging and troubleshooting

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

Function	Syntax	Log File
FortiNAC Server (Proxy RADIUS)	`nacdebug -name RadiusManager true`	/bsc/logs/output.master
FortiNAC Server (Local RADIUS)*	`nacdebug -name RadiusAccess true`	/bsc/logs/output.master
RADIUS Service (Local RADIUS)	`radiusd -X -l /var/log/radius/radius.log` Stop logging: Ctrl-C	/var/log/radius/radius.log
L2 related activity	`nacdebug -name BridgeManager true`	/bsc/logs/output.master
FortiGate wired port and Managed (FortiLink) FortiSwitch specific	`nacdebug -name Fortinet true`	/bsc/logs/output.master
FortiNAC Network association to each FortiGate	`nacdebug -name DeviceInterface true`	/bsc/logs/output.master
SSO activity**	`nacdebug -name SSOManager true`	/bsc/logs/output.master
Disable debug	`nacdebug -name <debug name> false`	N/A

*Enables logging for a given MAC Address:
```
nacdebug -logger 'yams.RadiusAccess.RadiusAccessEngine.00:11:22:33:44:55' -level FINEST
```

****SSO communication:**
As of version 8.8.5, logon and logoff messages are written to **/bsc/logs/output.master** in the FortiNAC CLI by default without debug enabled.

Logon Sample message:
FortiGate IP: 10.0.0.1
Client IP address: 10.0.0.10
Client MAC address = 00:09:B0:DA:40:C9
SSO Tag = Production

```
yams.SSOManager INFO :: 2021-02-23 07:33:25:003 :: SSOManager.sendMessage
sending message to 10.0.0.1 for client 00:09:B0:DA:40:C9
com.bsc.plugin.manager.SSOManager$DeviceMessage[logon,
mac=00:09:B0:DA:40:C9, ip=10.0.0.10, tags=[Production]]
```

Other Tools

Send a RADIUS Disconnect:
```
SendCoA -ip <devip> -mac <clientmac> -dis
```

Example:
```
SendCoA -ip 10.1.0.25 -mac 00:1B:77:11:CE:2F -dis
```

Manual SSO resync (versions 8.8.11 and greater)
```
SSOTool -r -ip <FortiGate IP>
```

Appendix

Connection Process

Network Connect

1. FortiNAC detects a device has connected
2. The device is evaluated against the existing Network Access Policies in FortiNAC.
3. FSSO Logon message is sent to FortiGate containing the following information:
   - IP Address
   - User ID – (logged on user, owner, or MAC address if userID is unknown)
   - Group: Group name or Firewall Tag name (determined by the matching Network Access Policy)
4. Based upon the received information, FortiGate applies the appropriate IPv4 Policy to the device.

Change

1. FortiNAC detects one of the following has changed:
   - Device status (e.g. Registered, Authenticated, Unauthenticated, At-Risk, Safe, - Disabled or Rogue)
   - Ownership ("Registered to")
   - User logon or logoff
   - IP Address

   Note: FortiNAC performs L2 Polls regularly and makes corrections as required. This includes changing the network access if the applied Network Access Policy no longer matches.

2. The device is re-evaluated against the existing Network Access Policies in FortiNAC.
3. If the matching policy has changed, FSSO message is sent to FortiGate containing the IP Address, User ID and updated Group
4. Based upon the received information, FortiGate applies the appropriate IPv4 Policy to the device.

Network Disconnect

1. FortiNAC detects the device has disconnected
2. FSSO Logon message is sent to FortiGate containing the IP Address, User ID and Group
3. FortiGate removes the group or firewall tag association and IPv4 Policy.

FortiGate CLI Access

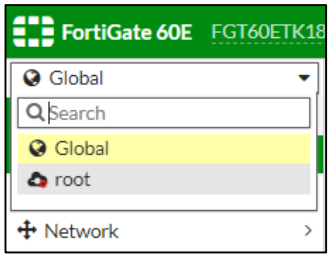
From FortiGate CLI:

The FortiGate UI can be used to initiate SSH sessions: click on the ">_" icon in the upper right corner of the page.

Security Fabric Connector and User Groups (FortiOS 6.0)

Fabric Connector

Note: If VDOM drop-down is available, select **root** VDOM (as opposed to Global)



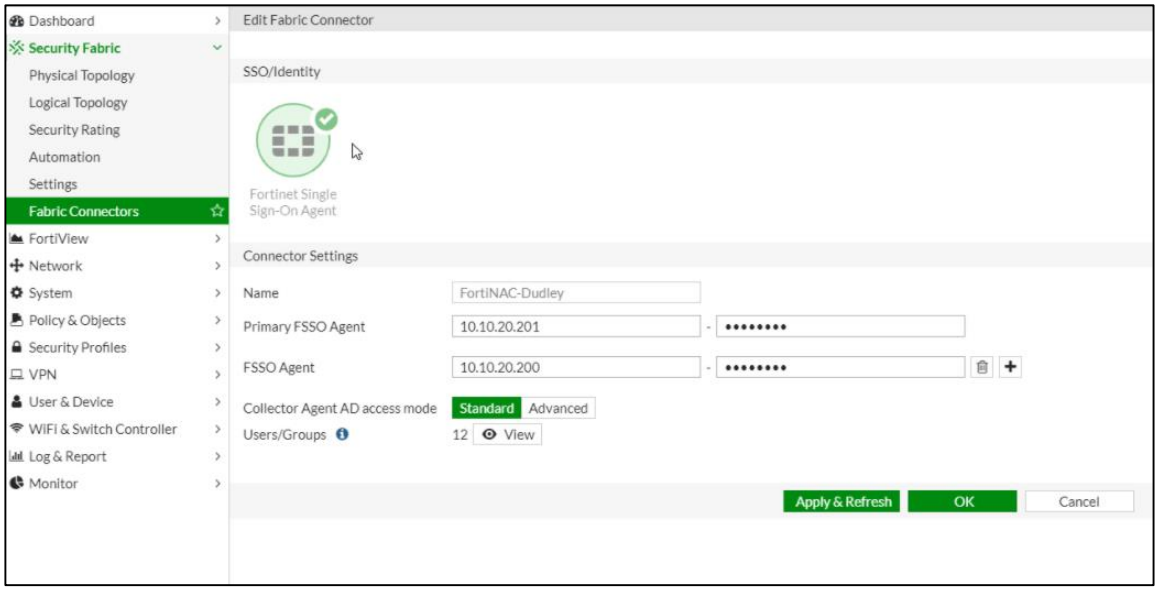
1. In the FortiGate UI, navigate to **Security Fabric > Fabric Connectors**
2. Click **Create New**
3. Click **Fortinet Single Sign-On Agent** icon
4. Configure using the chart below
5. Click **Apply & Refresh**

   Upon refresh, the number next to **Users/Groups** should update to reflect the number of Collector Agent Group Filters created. Click **View** to display the list of filters.

6. Click **OK**

Connector Settings

Name	Name of FortiNAC Server
Primary FSSO Agent	FortiNAC Server/Control server eth0 interface IP Address
Password	Must match the password used to configure Fortinet SSO Settings in FortiNAC
FSSO Agent (Click "+" to create)	**High Availability:** IP address of secondary control server (Do not use Shared IP address)
Password	Same value as Primary FSSO Agent password
Collector Agent AD Access Mode	Standard

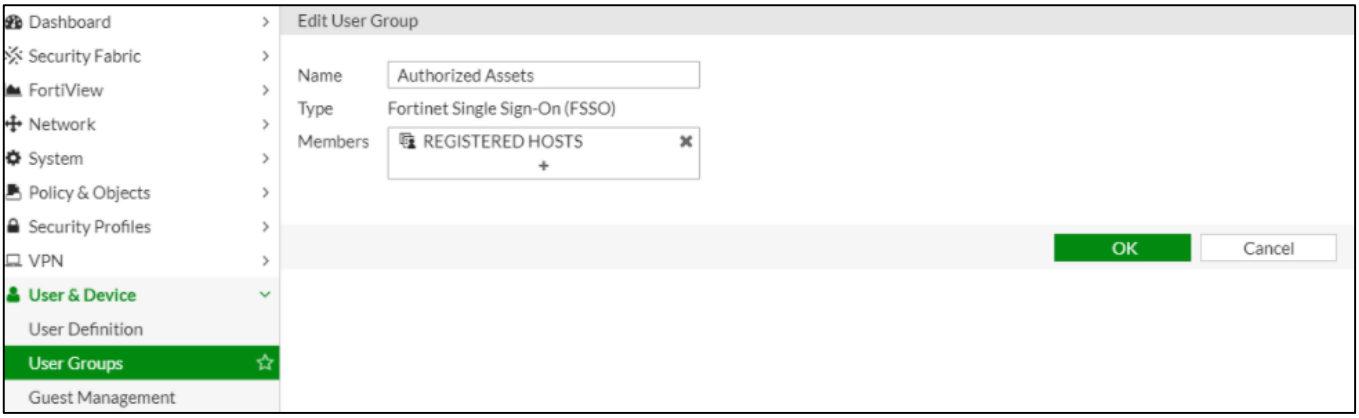


FSSO User Groups

1. In the FortiGate UI, navigate to **User & Device > User Groups**
2. Click **Create New**
3. Configure using chart below
4. Click **OK**
5. Proceed to Connecting Remote FortiGate and FortiNAC Over WAN Tunnel (if applicable). Otherwise, proceed to Firewall Policies.

User Group Settings

Name	Name of User Group
Type	Fortinet Single Sign-On (FSSO)
Members	Applicable FortiNAC User and/or Host group(s)

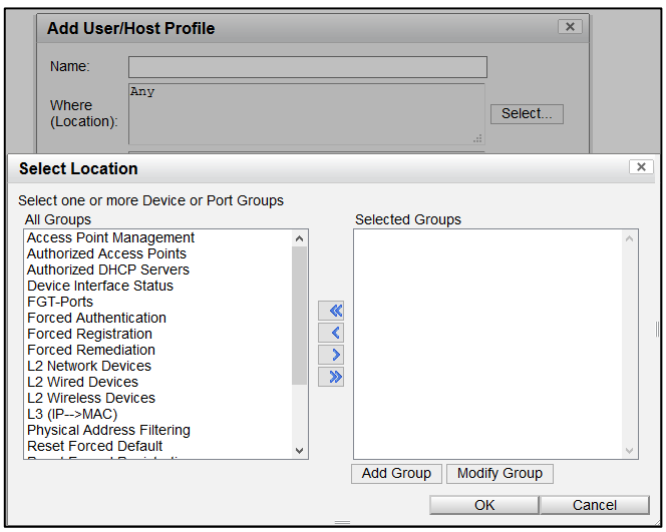


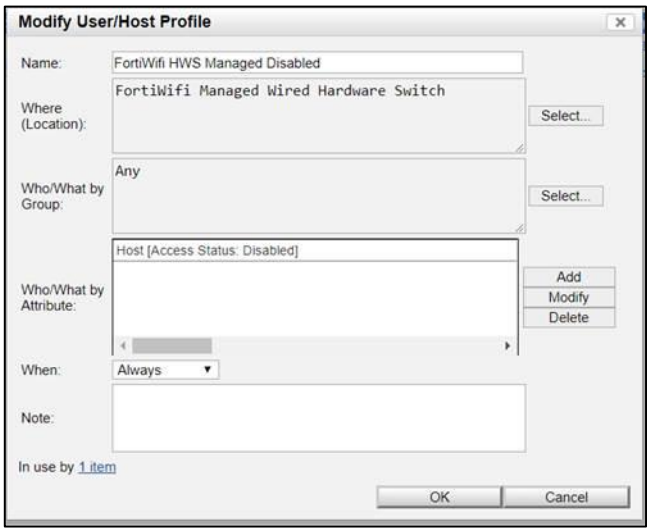
Network Access Policy Example (Direct Configuration)

Configure Policy

Navigate to **Policy > Policy Configuration**

1. Create a **User/Host Profile** to define the criteria for policy match.
   Important: The "Where" must include a port group containing the FortiGate interface created for the managed ports. The port group can be created by clicking **Select** next to **Where (Location)**.



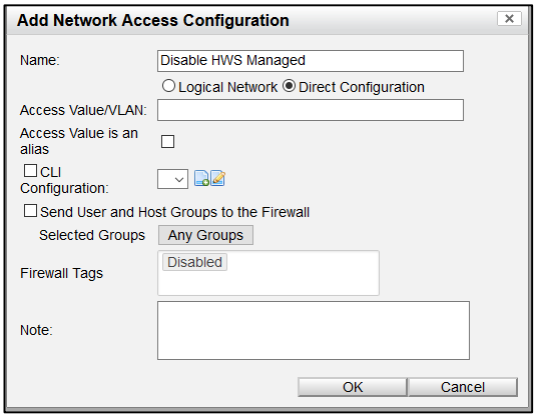


2. Create a **Network Access Policy** to assign the appropriate User/Host Group or Firewall Tag in the RADIUS response.

   Click **Direct Configuration**
   Select the groups or tags:

   User/Host Groups
   Select **Send User and Host Groups to the Firewall**
   Select the appropriate group and click the **>** button
   Click **OK**

   Firewall Tags
   Type the name of the tag in the Firewall Tags field

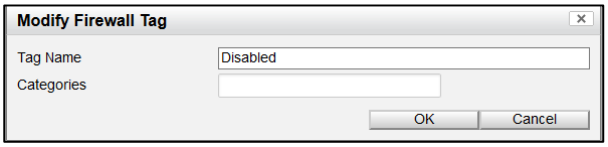


3. Rank policies accordingly.

Firewall Tags

If User or Host groups are not appropriate, create a Firewall Tag for the access value:

1. Navigate to **System > Settings > System Communication > Firewall Tags**
2. Click **Add**
3. Enter the Tag Name
4. Click **OK**



Proceed to Configure FortiGate.

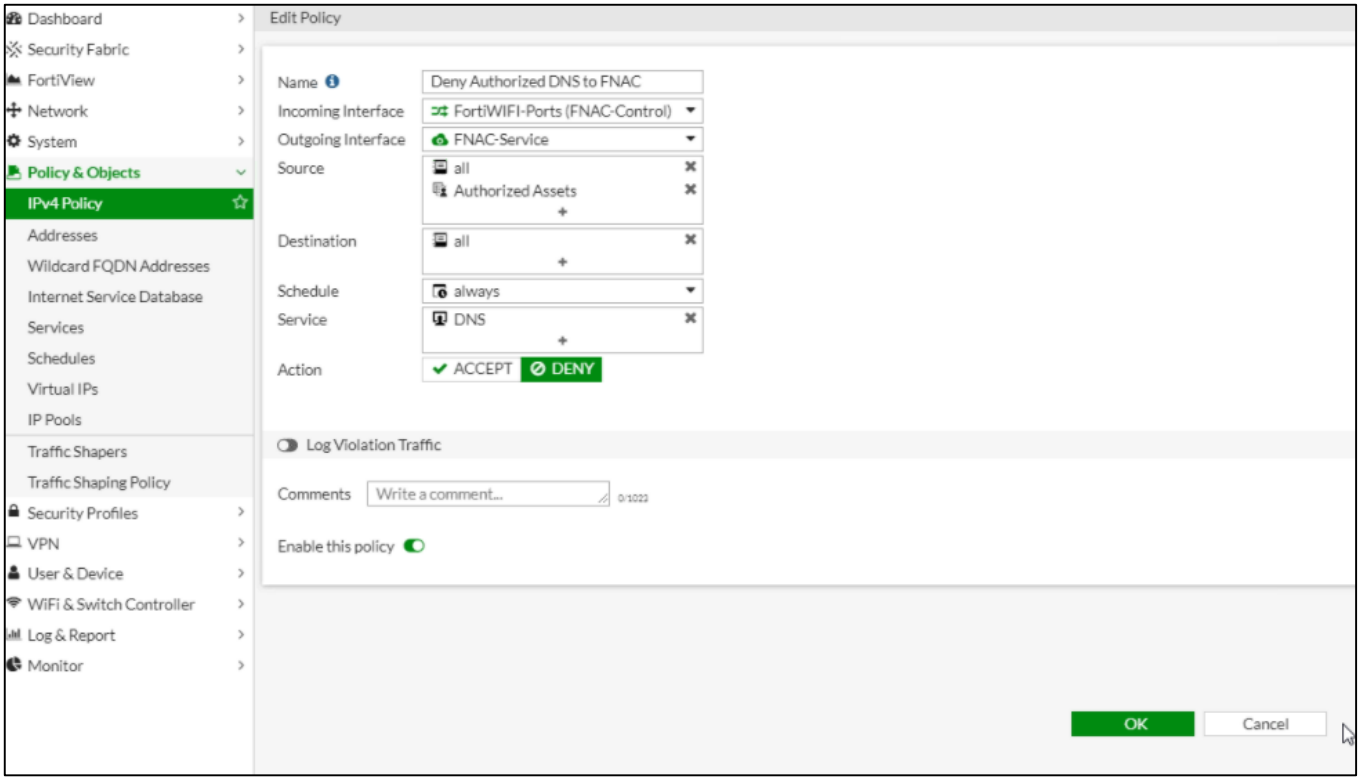
Firewall Policy Examples

Note: The following are examples. Policies will differ by network environment and organization requirements.

DNS for Authorized Hosts

Block authorized host DNS traffic to/from FortiNAC.

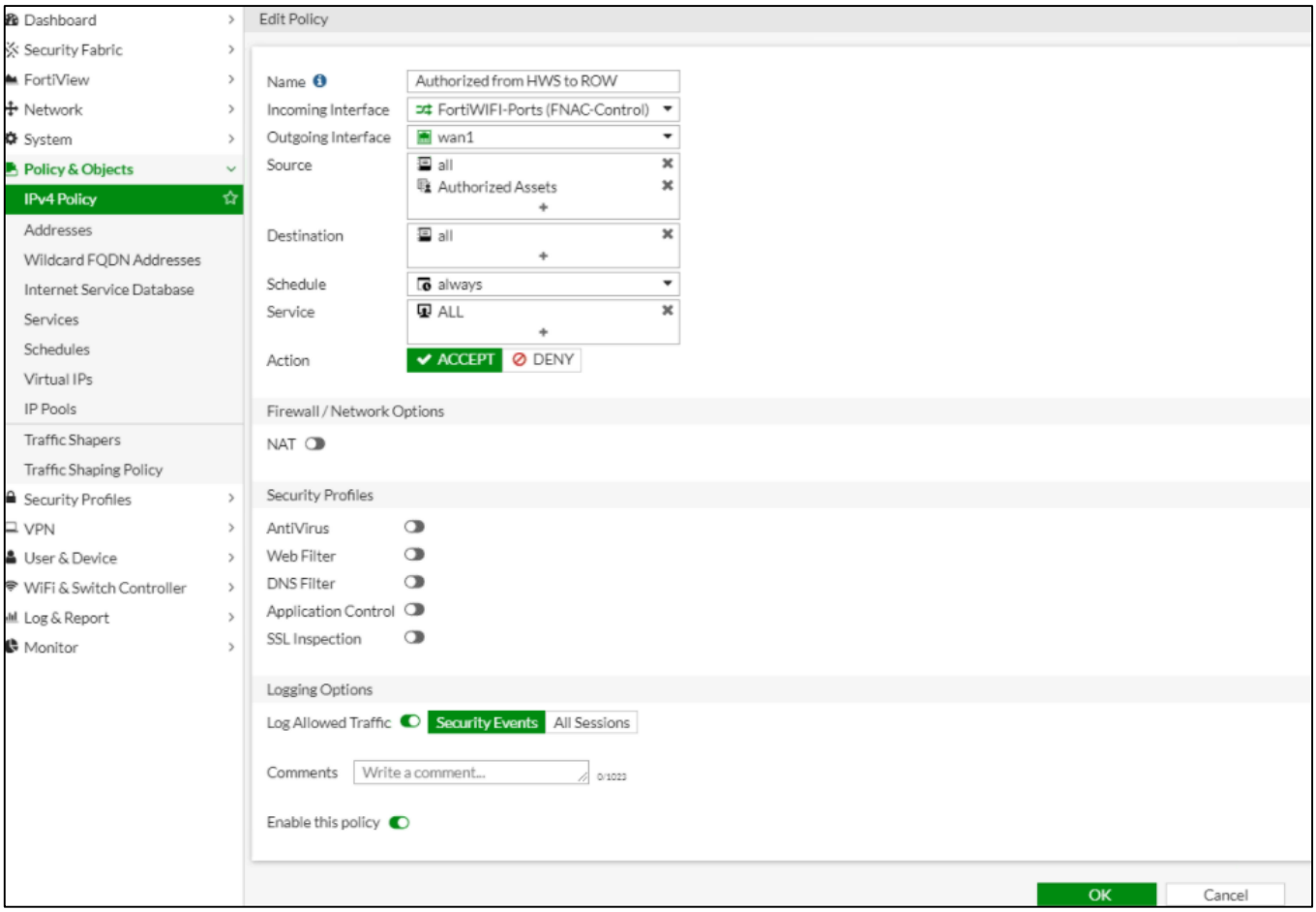
Name	Deny Authorized DNS to FortiNAC
Incoming Interface	Interface of managed ports
Outgoing Interface	FortiNAC interface
Source	All traffic Applicable User Group for registered hosts
Destination	All traffic
Schedule	Always
Service	DNS
Action	DENY
Enable this policy	enable



Network Access for Authorized Hosts

Allow authorized host traffic to/from the production network.

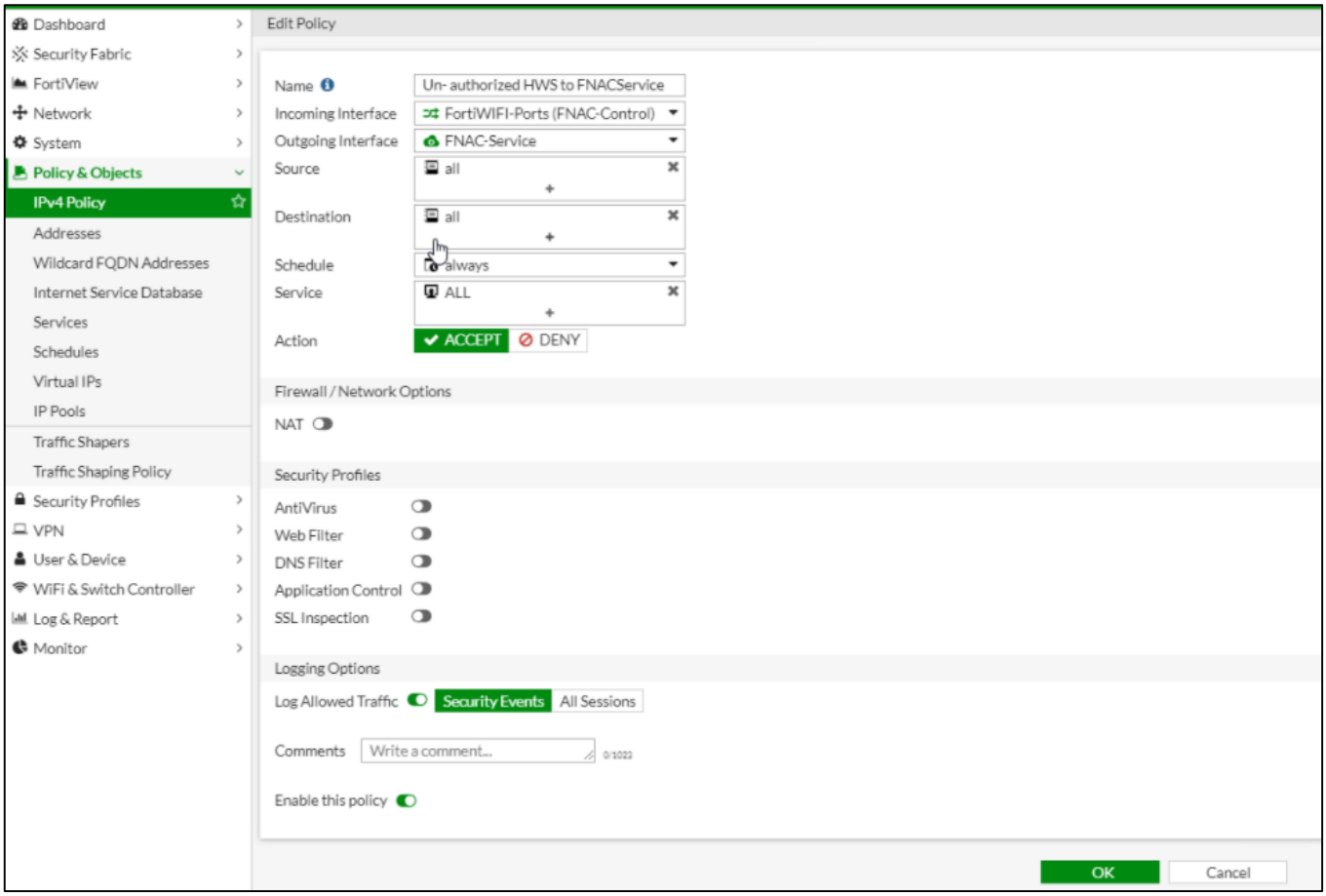
Name	Name of policy
Incoming Interface	Interface of managed ports
Outgoing Interface	wan
Source	All traffic Applicable User Group for registered hosts
Destination	All traffic
Schedule	Always
Service	ALL
Action	ACCEPT
NAT	May need to be enabled
Enable this policy	Enable



Network Access for Unauthorized Hosts

Allow unauthorized host traffic to/from FortiNAC.
Note: Another policy may be required to allow internet access for FortiNAC SSL certificate authentication as well as Anti-Virus/Anti-Spyware/Operating System remediation.

Name	Name of policy
Incoming Interface	Interface of managed ports
Outgoing Interface	FortiNAC interface
Source	All traffic
Destination	All traffic
Schedule	Always
Service	All
Action	ACCEPT
Enable this policy	enable



Network Access for Disabled Hosts (DeadEnd)

Disabled hosts are prevented from accessing the production network and are presented with the Captive Portal.

FortiNAC Network Access Policy

Firewall Tag: Disabled
User/Host Profile:

- **Where:** (Port group with FortiGate interface containing managed ports)
- **Who/What By Attribute:** Host: Access Status: Disabled

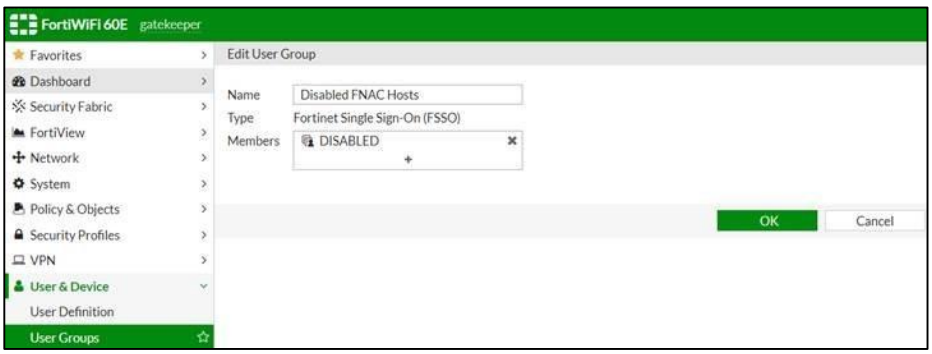
Network Access Configuration:

- **Direct Configuration**
- Firewall Tags: **Disabled**

Rank policy above the other policies for FortiGate Managed Ports.

Configure FortiGate Firewall Policy

1. Navigate to **Security Fabric > Fabric Connectors** – apply and refresh to pull in Disabled Tag created in FortiNAC
2. View User/Groups to see Disabled Tag was pulled in to FortiGate
3. Navigate to **User & Device > User Groups**
4. Create group type Fortinet Single Sign - On (FSSO) and add Disabled (tag pulled in from the Fabric Connector)



5. Navigate to **Policy and Objects > IPv4 Policy**
6. Create Policy to Control disabled hosts

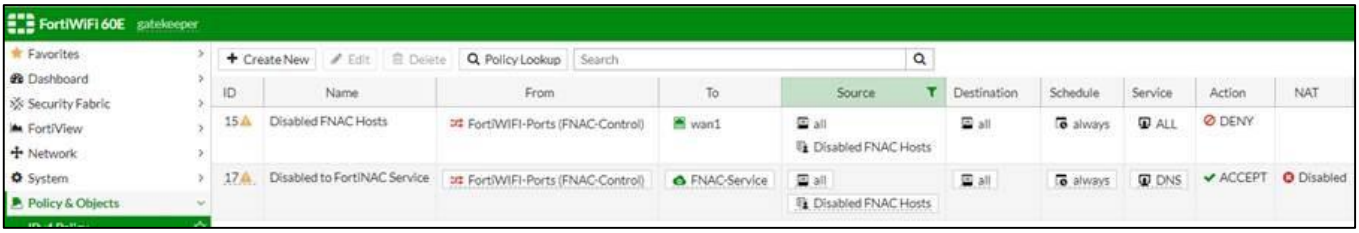
DeadEnd Network Access

Name	Name of policy
Incoming Interface	Interface of managed ports
Outgoing Interface	wan
Source	All traffic Disabled user group
Destination	All
Schedule	Always
Service	All
Action	DENY
Enable this policy	enable

DeadEnd DNS

Allow DNS traffic for disabled hosts to FortiNAC for Captive Portal access.

Name	Name of policy
Incoming Interface	Interface of managed ports
Outgoing Interface	FortiNAC interface
Source	All traffic Disabled user group
Destination	All
Schedule	Always
Service	DNS
Action	ACCEPT
Enable this policy	enable



Modify API Port

FortiNAC uses port 443 by default for REST API. To change the port FortiNAC uses for when communicating with the FortiGate, set the port to use through CLI:
`Device -setAttr -ip <FortiGate IP> -name API_Port -value <Port value>`

Example:
Device –setAttr –ip x.x.x.x –name API_Port –value 2222

```
************************ FWF60ETK18001734 ************************
Landscape = 207375981338 00:30:48:92:5B:1A
Pollable = true, Poll interval = 10 Minutes
Type = 1.3.6.1.4.1.12356.101.1.639
Group = 1.3.6.1.4.1.12356
MAC = null
Protocol = SnmpV1
Description =
IP = xxxx
State = Active
Status = Established
DBID = 8913
Attribute Count = 14
        Name = SnmpVersion value = 1 length = 1
        Name = CLI_CREDENTIALS value = CLICredentials
                User Name:[admin]
                Password:[***]
                Enable Password:[***]
                SessionType:[SSH2]
        Name = FirmwareVersion value = Fortigate36000 length = 14
        Name = SupportsVirtualization value = true length = 4
        Name = L2_ENABLED value = true length = 4
        Name = L2_POLL_DURATION value = 600 length = 3
        Name = L2_MIN_POLL_DURATION value = 300 length = 3
        Name = API_Port value = 2222 length = 3
        Name = 1.3.6.1.2.1.1.3.0 value = 58 days, 20:54:56.43 length = 20
        Name = userDefinedOID value = false length = 5
        Name = RestAPIVersion value = 0 length = 1
        Name = L2_LAST_POLL value = Mon Apr 01 08:23:24 EDT 2019 length = 28
        Name = L2_LAST_SUCCESSFUL_POLL value = Mon Apr 01 08:23:24 EDT 2019 length = 28
        Name = DEBUG value = ForwardingInterface length = 19
Community Strings: ********
```

Frequent L3 Polling Required for SSO

SSO is an IP Address-based type of enforcement. For accuracy, FortiNAC attempts to find the most recent up-to-date IP Address for the host. This is accomplished primarily by L3 polling the network infrastructure. It is normal operation for FortiNAC to L3 poll a FortiGate frequently when integrated using SSO.