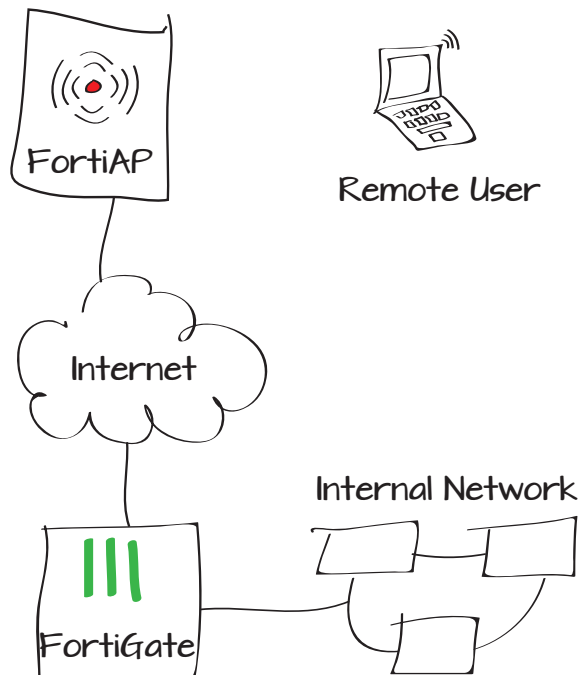


Providing remote users access to the corporate network and Internet

In this example, a user in a remote location, such as a hotel or their home, will use a FortiAP unit to securely connect to the corporate network and browse the Internet from behind the corporate firewall.

1. Preauthorizing the FortiAP unit on the FortiGate unit
2. Creating an SSID and firewall addresses
3. Creating security policies
4. Configuring the FortiAP unit to connect to the FortiGate unit
5. Connecting to the FortiGate unit remotely
6. Results



Pre-authorizing the FortiAP unit on the FortiGate unit

Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**.

Add a new FortiAP unit and enter the unit's **Serial Number** (in the example, *FAP11C3X13000412*).

The FortiAP unit will appear on the list of Managed FortiAPs as authorized and offline.'

Creating an SSID and a firewall addresses

Go to **WiFi Controller > WiFi Network > SSID**. Select **Create New**.

Enable the **DHCP Server** and make note of the IP range.

Configure the **WiFi Settings** with a unique **SSID** name and **Pre-shared Key**.

Serial Number:

Name:

Comments: 0/35

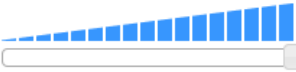
State: Authorized

Wireless Settings

Enable WiFi Radio

SSID: Automatically Inherit all SSIDs
 Select SSIDs

Auto TX Power Control: Disable Enable

TX Power:  100 %

Access Point	State	Connected Via	SSIDs	Channel
FAP11C3X13000412		-	Radio 1: All	Radio 1: 0

Name:

Type:

Traffic Mode:

IP/Network Mask:

Administrative Access: HTTPS PING HTTP FMG-Access
 SSH SNMP TELNET FCT-Access Auto IPsec Request

DHCP Server: Enable

Address Range:

Starting IP	End IP
10.80.10.100	10.80.10.254

Netmask:

Default Gateway: Same as Interface IP Specify

DNS Server: Same as System DNS Specify

Advanced...

WiFi Settings

SSID:

Security Mode:

Data Encryption: AES TKIP TKIP-AES

Pre-shared Key: (8 - 63 characters)

Go to **Firewall Objects > Address > Addresses**. Create addresses for both the remote users and the corporate network.

For the remote users, set **Type** to **IP Range**. The range for the remote users should be within the range used for the DHCP server. Set **Interface** to the new SSID.

For the corporate network, set **Type** to **Subnet** and use the corporate network's IP address. Set **Interface** to an internal interface.

Creating security policies

Go to **Policy > Policy > Policy**.

Create a policy that allows remote wireless users to access the Internet. Set the **Incoming Interface** to the SSID and the **Outgoing Interface** as your Internet-facing interface.

Category Address IPv6 Address

Name

Type

Subnet / IP Range

Interface

Show in Address List

Comments 0/255

Category Address IPv6 Address

Name

Type

Subnet / IP Range

Interface

Show in Address List

Comments 0

Policy Type Firewall VPN

Policy Subtype Address User Identity Device Identity

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service

Action

Enable NAT

Use Destination Interface Address Fixed Port

Use Dynamic IP Pool

Logging Options

No Log

Log Security Events

Log all Sessions

Create a second policy for remote wireless users to access the corporate network. Again, set the **Incoming Interface** to the SSID but now the **Outgoing Interface** is an internal interface.


Configuring the FortiAP unit to connect to the corporate FortiGate unit


Go to **WiFi Controller > Managed Access Points > Managed FortiAPs** and note the IP Address assigned to your FortiAP.


Enter the address into your browser's address bar to access your FortiAP web manager.


Policy Type: Firewall VPN


Policy Subtype: Address User Identity Device Identity


Incoming Interface: WLAN_1 (SSID: RemoteWiFi) 


Source Address: Wireless_Users 

Outgoing Interface: internal 

Destination Address: Corp_Network 

Schedule: always 

Service: ALL 

Action: ACCEPT 

Enable NAT

Use Destination Interface Address Fixed Port



Use Dynamic IP Pool

Logging Options

No Log

Log Security Events

Log all Sessions

Access Point	State	Connected Via	SSIDs
FAP11C3X13000412		 10.10.10.2	Radio 1: All

In the **System Information** tab, enter the **AC IP Address** of the public facing interface of the corporate FortiGate unit. The Internet-facing interface is also the public facing interface. To locate this IP address, go to **System > Network > Interfaces**.

The FortiAP will search for this FortiGate interface when it tries to connect.

The remote user may now take this device to the desired remote location to connect securely to the corporate FortiGate unit.

Connecting to the corporate FortiGate remotely

At the remote location, connect the FortiAP to the Internet using an Ethernet cable. Next, connect the FortiAP to power.

Once connected, the FortiAP requests an IP address and locates the FortiGate wireless controller.

The remote user can now access the corporate network and browse the Internet securely from behind the corporate firewall.

AC Discovery Type	<input checked="" type="radio"/> Auto <input type="radio"/> Static <input type="radio"/> DHCP <input type="radio"/> DNS <input type="radio"/> Broadcast <input type="radio"/> Multicast
AC Control Port	<input type="text" value="5246"/>
AC IP Address 1	<input type="text" value="172.20.120.141"/>
AC IP Address 2	<input type="text"/>
AC IP Address 3	<input type="text"/>
AC Host Name 1	<input type="text" value="_capwap-control._udp."/>
AC Host Name 2	<input type="text"/>
AC Host Name 3	<input type="text"/>
AC Discovery Multicast Address	<input type="text" value="224.0.1.140"/>
AC Discovery DHCP Option Code	<input type="text" value="138"/>
AC Data Channel Security	<input type="radio"/> Clear Text <input type="radio"/> DTLS Enabled <input checked="" type="radio"/> Clear Text or DTLS Enabled

Results

Go to **WiFi Controller > Monitor > Client Monitor** to see remote wireless users connected to the FortiAP unit.

Go to **Log & Report > Traffic Log > Forward Traffic** to see remote wireless users appear in the logs.

Select an entry to view more information about remote traffic to the corporate network and to the Internet.

Device	Auth	IP	FortiAP	SSID	Channel	Bandwidth Tx/Rx	Signal
84:29:99:be:54:dc	Pass	10.80.10.100	FortiAP 220B (1)	RemoteWiFi	44	0 Kbps	
70:f1:a1:54:f6:27	Pass	10.80.10.103	FortiAP 220B (2)	RemoteWiFi	6	47 Kbps	

#	Date/Time	Device	Src	Dst	Src Interface	Dst Interface	Policy ID	Bytes
1	3 seconds ago		10.80.10.103	213.199.179.151	WLAN_1	wan1	10	172
2	4 seconds ago		10.80.10.103	157.55.130.147	WLAN_1	wan1	10	176
3	3 seconds ago		10.80.10.103	172.20.120.235	WLAN_1	wan1	10	140
4	4 seconds ago		10.80.10.103	207.112.47.253	WLAN_1	wan1	10	435
5	6 seconds ago		10.80.10.103	172.20.181.253	WLAN_1	wan1	10	0 B
6	8 seconds ago		10.80.10.103	192.168.1.112	WLAN_1	internal	6	0 B
7	8 seconds ago		10.80.10.101	173.194.76.109	WLAN_1	wan1	10	12...

Dst	192.168.1.112	Virtual Domain	root
Received	0	Source Country	Reserved
Src NAT IP	192.168.1.99	Sent / Received	0 B / 0 B
Duration	0	Sent	0
Src NAT Port	55873	Application Details	
Service	RDP	Protocol	6
Destination Country	Reserved	Dst Port	3389
roll	65528	Status	start
Timestamp	Wed Nov 7 10:20:54 2012	Sequence Number	195221
Policy ID	6	Src Interface	WLAN_1
Src	10.80.10.103	Level	notice
Src Port	55873	logid	15
Sub Type	forward	Threat	
Tran Display	snat	Date/Time	8 seconds ago (Wed Nov 7 10:20:54 2012)
Dst Interface	internal		

Dst	157.55.130.147	Virtual Domain	root
Received	102	Source Country	Reserved
Src NAT IP	172.20.120.123	Sent / Received	176 B / 102 B
Duration	181	Sent	176
Src NAT Port	37023	Application Details	
Service	40046/udp	Protocol	17
Destination Country	United States	Dst Port	40046
roll	65528	Status	accept
Timestamp	Wed Nov 7 10:20:58 2012	Tran Display	snat
Sequence Number	194834	Policy ID	10
Src Interface	WLAN_1	Src	10.80.10.103
Sent Packets	1	Level	notice
Src Port	37023	logid	13
Sub Type	forward	Threat	
Received Packets	1	Date/Time	4 seconds ago (Wed Nov 7 10:20:58 2012)
Dst Interface	wan1		