

Requisitos para conectar AP's a la red del MI

Requisitos Generales

- 1) Tener un Controlador de AP's (CAP) gestionado por usuarios Administradores locales y/o LDAP y/o Radius, con permisos para:
 - a) Habilitar/quitar/modificar los AP's de la red al igual que los Routers
 - b) Crear/Modificar/Quitar usuarios administradores con diferentes niveles de permisos.
 - c) Definir VPN IPSec Site-to-Site en el Router y rutear todo el tráfico por allí.
 - d) Brindar más de un DHCP local (usuarios, invitados) o hacer DHCP Relay.
 - e) Configurar cliente Radius para validar acceso a los AP
 - f) Configurar y brindar SSID de invitados mediante Tokens o Vouchers temporales definidos.
 - g) Generar desde usuarios Administradores limitados, los Tokens o Vouchers temporales a ser entregados a los invitados.
 - h) Limitar el acceso a ciertas redes definidas por el Administrador Global.
 - i) Definir red LAN
 - j) Definir red WAN
 - k) Configurar Hotspot donde se validen los usuarios contra AD/Radius

- 2) Requisitos AP
 - a) Soporte para 802.11a/b/g/n/ac
 - b) Doble banda 2.5 Ghz y 5 Ghz
 - c) 802.3af/A PoE & 24V PoE
 - d) Debe traer base de montaje
 - e) Los AP's no podrán configurarse sin el CAP
 - f) Diseño compacto y discreto, entre 160mm y 200mm
 - g) 1 Puerto 100/1000 Ethernet

- 3) Requisitos Gateway Router
 - a) Más de 3 interfaces Gigabit LAN
 - b) Interface de PoE out
 - c) SNMP
 - d) NTP
 - e) Permitir IPSec site-to-site, con las siguientes configuraciones de seguridad como mínimo:
 - 1) Fase 1 y 2
 - 2) IKE Version 1 y/o 2
 - 3) Encriptado AES256
 - 4) Autenticación SHA1
 - 5) DH group: 14

Al conectar el AP se establece una VPN IPSec site-to-site contra FortiGate3100D, sin esto no debe funcionar.

Pasos:

- 1) Seleccionar el SSID a conectarse
- 2) Se ingresa usuario y clave, y se valida contra el AD mediante un servidor Radius
- 3) Si es un usuario válido*, se finaliza el proceso y se conecta el dispositivo al AP y se asigna una IP
- 4) Al intentar navegar:
 - a) Se volverá a solicitar un usuario y clave y navegará con los permisos que este tenga.
Necesita configurarse un proxy
 - b) No se solicitará usuario y clave.
Tendrá navegación directa. Para limitar esto se debe definir previamente un rango de IP a asignar por los APs y tener un grupo de navegación limitado asociado a la misma.

Pasos invitados:

- 1) El Administrador local ingresa al CAP y genera un Token o Voucher temporal
- 2) El Invitado selecciona el SSID a conectarse
- 3) Se pide que ingrese el Token o Voucher temporal, si es válido, se finaliza el proceso y se conecta el dispositivo al AP y se asigna una IP, el mismo permanecerá conectado por el tiempo que se haya definido.
Tendrá navegación directa. Para limitar esto se debe definir previamente un rango de IP a asignar por los APs para los invitados y tener un grupo de navegación limitado asociado a la misma.

****IMPORTANTE: A tener en cuenta que si las credenciales son correctas el logueo es muy rápido, en cambio si no son correctas las credenciales puede demorar unos minutos intentando conectarse y luego dará el mensaje de error.***

ANEXO

Requisitos AP's red del MI

Requisitos Generales

- 1) Controlador de AP's (CAP) centralizado, gestionado por usuarios Administradores locales y/o LDAP y/o Radius, con permisos para:
 - a) Habilitar/quitar/modificar los AP's de la red al igual que los Routers
 - b) Crear/Modificar/Quitar usuarios administradores con diferentes niveles de permisos.
 - c) Definir VPN IPSec Site-to-Site en el Router y rutear todo el tráfico por allí.
 - d) Brindar más de un DHCP local (usuarios, invitados) o hacer DHCP Relay.
 - e) Configurar cliente Radius para validar acceso a los AP
 - f) Configurar y brindar SSID de invitados mediante Tokens o Vouchers temporales definidos.
 - g) Generar desde usuarios Administradores limitados, los Tokens o Vouchers temporales a ser entregados a los invitados.
 - h) Limitar el acceso a ciertas redes definidas por el Administrador Global.
 - i) Definir red LAN
 - j) Definir red WAN
 - k) Configurar Hotspot donde se validen los usuarios contra AD/Radius

- 2) Requisitos AP
 - a) Soporte para 802.11a/b/g/n/ac
 - b) Doble banda 2.5 Ghz y 5 Ghz
 - c) 802.3af/A PoE & 24V PoE
 - d) Debe traer base de montaje
 - e) Los AP's no podrán configurarse sin el CAP
 - f) Diseño compacto y discreto, entre 160mm y 200mm
 - g) 1 Puerto 100/1000 Ethernet

- 3) Requisitos Security Gateway Router
 - a) Más de 3 interfaces Gigabit LAN
 - b) Interface de PoE out
 - c) SNMP
 - d) NTP
 - e) Permitir IPSec site-to-site, con las siguientes configuraciones de seguridad como mínimo:
 - 1) Fase 1 y 2
 - 2) IKE Version 1 y/o 2
 - 3) Encriptado AES256
 - 4) Autenticación SHA1
 - 5) DH group: 14