

SonicWall

Configuração CtrlSpot no SonicWall

Tutorial técnico para integração do captive portal **CtrlSpot** com firewalls **SonicWall** (SonicOS 6.5 / 7.x), utilizando autenticação externa via portal hospedado e RADIUS.

“ **Observação:** Os parâmetros sensíveis (*shared secret*, portas RADIUS específicas e eventuais credenciais administrativas) serão enviados diretamente ao cliente por canal seguro. Onde aparecer `<SHARED_SECRET>` ou `<PORTA>`, substitua pelos valores fornecidos.

1. Pré-requisitos

Antes de iniciar, confirme:

- Acesso administrativo à interface web do SonicWall.
- SonicOS 6.5.x ou 7.x (os menus variam ligeiramente entre versões — ambos cobertos abaixo).
- A zona/interface de Wi-Fi de visitantes já criada (ex.: zona `WLAN` ou interface dedicada a guests).
- Conectividade de saída do firewall para o portal e o RADIUS.
- Resolução DNS funcional para os hosts do CtrlSpot.

Dados da solução

Item	Valor
Endereço do portal	<code>captive.[cliente].ctrlspot.com</code>
Servidor RADIUS	<code>radius-3.lab3.co</code>
Shared secret RADIUS	<code><SHARED_SECRET></code> (<i>enviado ao cliente</i>)

Item	Valor
Porta de autenticação RADIUS	<PORTA_AUTH> (enviado ao cliente, padrão 1812)
Porta de accounting RADIUS	<PORTA_ACCT> (enviado ao cliente, padrão 1813)

2. Liberações de rede necessárias

O firewall e os clientes precisam alcançar a infraestrutura CtrlSpot. Garanta as seguintes liberações de saída:

Origem	Destino	Porta/Protocolo	Finalidade
Zona de guests	captive.[cliente].ctrlspot.com	TCP 443 (HTTPS)	Redirecionamento e exibição do portal
Firewall	radius-3.lab3.co	UDP <PORTA_AUTH>	Autenticação RADIUS
Firewall	radius-3.lab3.co	UDP <PORTA_ACCT>	Accounting RADIUS
Zona de guests	DNS interno/externo	UDP 53	Resolução do host do portal

“ É recomendável criar **Address Objects** para os hosts do CtrlSpot e do RADIUS, facilitando o reuso em regras e políticas de *walled garden* (acesso permitido antes da autenticação).

3. Criar o objeto do servidor RADIUS

SonicOS 7.x

1. Acesse **Device → Users → Settings**.
2. Em **User authentication method**, selecione **RADIUS** (ou **RADIUS + Local Users** se desejar fallback local).
3. Clique em **Configure RADIUS**.
4. Aba **Settings**, clique em **Add** e preencha:
 - **Name/IP Address:** radius-3.lab3.co
 - **Port:** <PORTA_AUTH>
 - **Shared Secret / Confirm Secret:** <SHARED_SECRET>
5. Aba **RADIUS Users**: defina o mecanismo de mapeamento de grupos (use **Use RADIUS Filter-Id attribute** se a CtrlSpot enviar grupos via Filter-Id).
6. Aba **Test**: valide a conectividade com um usuário de teste antes de prosseguir.

SonicOS 6.5

1. Acesse **Manage** → **Users** → **Settings**.
2. Em **Authentication method for login**, selecione **RADIUS** ou **RADIUS + Local Users**.
3. Clique em **Configure RADIUS** e repita os mesmos campos acima (host, porta, shared secret, accounting).

“ Configure também o **accounting** apontando para `radius-3.lab3.co` na porta `<PORTA_ACCT>` — a CtrlSpot usa accounting RADIUS para controle de sessão, tempo de uso e desconexão.

4. Criar a Custom Authentication Page (redirecionamento ao portal externo)

O SonicWall precisa redirecionar o usuário não autenticado para a URL externa do CtrlSpot.

1. Acesse **Device** → **Users** → **Settings** (7.x) ou **Manage** → **Users** → **Settings** (6.5).
2. Localize a seção **Customize Login Pages / Authentication Pages**.
3. Em **External guest authentication** (ou ao editar a página de login da zona), defina:
 - **Login redirect / Web server host name:** `captive.[cliente].ctrlspot.com`
 - **Protocol:** `HTTPS`
 - **Port:** `443`
4. Salve.

Esse host será o destino para onde o cliente é enviado quando tentar navegar sem sessão ativa.

5. Configurar Guest Services e o Captive Portal na zona

5.1 Criar/editar a zona Wi-Fi de visitantes

1. Acesse **Network** → **Zones** (7.x) ou **Manage** → **Network** → **Zones** (6.5).
2. Edite a zona usada pelos guests (ex.: `WLAN`).
3. Marque **Enable Guest Services**.

4. Clique em **Configure** (Guest Services).

5.2 Opções de Guest Services

Na janela de Guest Services, configure:

- **Enable External Guest Authentication** — habilita o uso de um portal/servidor externo.
- **Web Server Host Name:** `captive.[cliente].ctrlspot.com` (HTTPS, porta 443).
- **RADIUS Server:** selecione o servidor `radius-3.lab3.co` criado na etapa 3.
- **Pass Networks / Walled Garden:** adicione os Address Objects de `captive.[cliente].ctrlspot.com` e demais domínios exigidos pela CtrlSpot, para que carreguem **antes** da autenticação (logo, termos, CSS/JS, gateways de pagamento se aplicável).
- **Session Idle Timeout / Max Session:** ajuste conforme política do cliente (ou deixe que o RADIUS controle via atributos).
- **Redirect SMTP traffic / Deny networks:** opcional, conforme política.

5.3 Aplicar à interface/SSID

Garanta que a interface (ou o SSID, no caso de SonicWave/SonicPoint) está atribuída a essa zona com Guest Services ativo.

6. Fluxo de autenticação esperado

1. Cliente conecta-se ao SSID de visitantes e recebe IP via DHCP do SonicWall.
 2. Ao tentar navegar, o SonicWall intercepta a sessão (usuário não autenticado).
 3. O usuário é redirecionado para `https://captive.[cliente].ctrlspot.com`, recebendo parâmetros do gateway (MAC do cliente, IP do gateway, URL original).
 4. O usuário autentica-se na página CtrlSpot (login social, voucher, SMS, etc.).
 5. A CtrlSpot valida e devolve a sessão ao SonicWall via RADIUS (`radius-3.lab3.co`).
 6. O SonicWall libera a navegação e inicia o **accounting** RADIUS da sessão.
 7. Encerramento de sessão por timeout, logout ou desconexão (CoA/Disconnect quando suportado).
-

7. Validação e testes

- **Teste de RADIUS:** use a aba **Test** em Configure RADIUS com um usuário válido — espera-se `Authentication succeeded`.

- **Teste de redirecionamento:** conecte um dispositivo ao SSID de guests e abra um site HTTP — deve redirecionar ao portal CtrlSpot.
- **Walled garden:** confirme que o portal carrega completamente (imagens, scripts) sem autenticação prévia.
- **Sessão ativa:** após autenticar, verifique em **Users → Status** (ou **Investigate → Logs → Users**) se a sessão aparece como autenticada com o usuário correto.
- **Accounting:** confirme no painel CtrlSpot que start/stop de accounting estão chegando.

8. Troubleshooting

Sintoma	Causa provável	Ação
Não há redirecionamento	Guest Services / External Guest Auth desabilitado na zona	Reveja etapa 5
Redireciona mas portal não carrega	Domínios CtrlSpot fora do walled garden	Adicione os Address Objects em Pass Networks
Portal carrega mas login falha	Shared secret ou porta RADIUS incorretos	Reveja etapa 3 e os dados enviados ao cliente
Autentica mas não libera navegação	Resposta RADIUS sem atributo de aceitação esperado / accounting bloqueado	Verifique liberação UDP <PORTA_ACCT> e atributos de retorno
Erro de certificado no portal	HTTPS/host name divergente do certificado	Confirme o host captive.[cliente].ctrlspot.com exato em Web Server Host Name
Sessão cai cedo demais	Idle/Max session muito baixos	Ajuste em Guest Services ou via atributos RADIUS

Logs úteis

- **Monitor → Logs / Investigate → Logs** — eventos de autenticação, RADIUS e Guest Services.
- Filtre por categoria **Users** e **Security Services** para isolar falhas de RADIUS e redirecionamento.

9. Checklist final

- [] Servidor RADIUS configurado (auth + accounting) com shared secret correto
- [] Host do portal definido em HTTPS/443
- [] Guest Services + External Guest Authentication habilitados na zona de visitantes

- [] Walled garden / Pass Networks contemplando os domínios CtrlSpot
 - [] Teste de RADIUS com sucesso
 - [] Redirecionamento ao portal validado
 - [] Sessão autenticada e accounting confirmados no painel CtrlSpot
-

Revisão #1

Criado 9 junho 2026 00:46:23 por Felipe Weckx

Atualizado: 9 junho 2026 00:46:57 por Felipe Weckx