

Guia de atualização do SonicWall™ SonicOS 6.2

Maio de 2017

Este Guia de atualização fornece instruções para atualizar o seu dispositivo de segurança de rede SonicWall™ do SonicOS 6.1 ou uma versão anterior do SonicOS 6.2 para a última versão do SonicOS 6.2.

i **NOTA:** Este documento pode conter descrições sobre uma plataforma/versão que não foi lançada em determinados países ou regiões.

Este guia fornece também informações sobre a importação das definições de configuração a partir de um dispositivo funcionando com SonicOS 5.8, 5.9, 6.1 ou 6.2 para um dispositivo funcionando com SonicOS 6.2. Consulte [Importar as definições de configuração](#) para obter detalhes sobre os modelos e as versões de firmware compatíveis.

Tópicos:

- [Obter a versão mais recente de firmware do SonicOS](#)
- [Criar um backup do sistema e exportar as suas configurações](#)
- [Atualizar firmware com as configurações atuais](#)
- [Atualizar firmware com as configurações padrão de fábrica](#)
- [Uso do Modo de segurança para atualizar o firmware](#)
- [Sobre atualizações e túneis VPN](#)
- [Importar as definições de configuração](#)

⚠ CUIDADO: No SuperMassive™ 9800, você poderá precisar atualizar as versões do ChassisOS e do FailSafe antes de instalar a versão 6.2.1.3 ou superior do SonicOS. Você pode ver estas versões no Modo de segurança. Consulte as notas de versão do SonicOS 6.2.1.x para saber as versões necessárias. Entre em contato com o suporte técnico da SonicWall antes de atualizar o seu dispositivo SuperMassive 9800 se estas versões estiverem desatualizadas.

i **NOTA:** A partir do SonicOS 6.2.5.0, todos os certificados padrão do SonicOS são atualizados para criptografia de 2048 bits/SHA-256, exceto o Certificado de CA de DPI-SSL da SonicWall padrão que é atualizado a partir do SonicOS 6.2.5.1. Após atualizar o seu dispositivo para a versão 6.2.5 ou superior, siga um dos seguintes procedimentos, ou ambos, para substituir os antigos certificados de 1024 bits pelos novos:

- Navegue até a página Sistema > Administração, role para baixo até **Configurações de gerenciamento da Web** e clique no botão **Gerar certificado**. Isso regenera o certificado de gerenciamento HTTPS autoassinado.
- Navegue até a página Sistema > Configurações, clique em **Exportar configurações** para salvar uma cópia de suas definições de configuração e, em seguida, clique no ícone Inicializar na linha de **Firmware atual com configurações padrão de fábrica**. Esta ação vai regenerar todos os certificados padrão. Após a reinicialização, clique no botão **Importar configurações** para importar suas configurações e retornar à sua configuração anterior.

Obter a versão mais recente de firmware do SonicOS

Para obter um novo arquivo de imagem de firmware do SonicOS para seu dispositivo de segurança SonicWall:

- 1 Em um navegador de seu computador de gerenciamento, faça logon em sua conta MySonicWall em <http://www.mysonicwall.com>.
- 2 Em MySonicWall, clique em **Downloads** no painel de navegação esquerdo para exibir a tela Centro de download.
- 3 Selecione seu produto na lista suspensa **Tipo de software** para exibir as versões de firmware disponíveis.
- 4 Para baixar o firmware para seu computador, clique no link da versão de firmware que deseja. Você pode fazer download das *Notas de versão* e de outros arquivos associados da mesma forma.

Criar um backup do sistema e exportar as suas configurações

Antes de iniciar o processo de atualização, crie um backup do sistema em seu dispositivo SonicWall.

Nos dispositivos SonicWall das séries NSA e SuperMassive 9000, o recurso de backup salva uma cópia do estado atual do sistema, do firmware e das definições de configuração em seu dispositivo, protegendo todas as suas configurações existentes caso se torne necessário regressar a um estado de configuração anterior.

Em aplicativos SonicWall das séries TZ e SOHO Wireless, você pode criar um backup das suas definições de configuração atuais no dispositivo, para usar com a versão de firmware atual ou com uma versão de firmware recentemente carregada.

Também é possível exportar as definições de configuração do dispositivo para um arquivo na sua estação de gerenciamento local. Esse arquivo serve de backup externo das definições de configuração e pode ser importado para outro dispositivo ou para o mesmo dispositivo caso seja necessário reiniciar o firmware com as configurações padrão de fábrica.

Para salvar um backup do sistema em seu dispositivo e exportar as definições de configuração para um arquivo em sua estação de gerenciamento local:

- 1 Na página Sistema > Configurações, siga um dos seguintes procedimentos:
 - Em um dispositivo SuperMassive ou NSA, clique em **Criar backup**. O SonicOS tira um "instantâneo" do estado do sistema, do firmware e das preferências de configuração atuais que formarão a nova imagem de firmware do Backup do sistema. Clicar em **Criar backup** irá substituir a imagem de Backup do sistema que exista. A entrada **Backup do sistema** é exibida na tabela Gerenciamento de firmware.
 - Em um dispositivo TZ ou SOHO W, clique em **Criar configurações de backup**. O SonicOS salva um pequeno arquivo no dispositivo com todas as suas definições de configuração. Qualquer arquivo de definições de backup anterior é substituído. A tabela de Gerenciamento de firmware exibe a entrada **Firmware atual com configurações de backup**.

i **NOTA:** É exibido um botão de **Download** na tabela de Gerenciamento de firmware para o arquivo de Backup do sistema e de Configurações de backup. No entanto, os arquivos baixados não podem ser importados para outro dispositivo, nem podem ser carregados como firmware. Use **Exportar configurações** para salvar as suas definições de configuração para importação noutro dispositivo.

- 2 Para exportar as suas configurações para um arquivo local, clique em **Exportar configurações** e, em seguida, clique em **Exportar** na janela pop-up que exibe o nome do arquivo salvo.

Atualizar firmware com as configurações atuais

Você pode atualizar a imagem do SonicOS em um dispositivo de segurança SonicWall remotamente se a interface LAN ou WAN estiver configurada para acesso de gerenciamento. Em plataformas SonicWall NSA ou SuperMassive, é possível conectar-se diretamente à porta MGMT e direcionar o seu navegador para esse endereço IP (<http://192.168.1.254> por padrão) para efetuar login e executar a atualização.

Para carregar firmware novo para seu dispositivo SonicWall e usar suas definições de configuração atuais na inicialização:

- 1 Baixe o arquivo de imagem de firmware do SonicOS a partir do MySonicWall e salve-o em seu computador local.
- 2 Direcione seu navegador para o endereço IP do dispositivo e efetue login como administrador.
- 3 Na página Sistema > Configurações, clique em **Carregar novo firmware**.
- 4 Navegue até o local onde salvou o arquivo de imagem de firmware do SonicOS, selecione o arquivo e clique em **Carregar**. Após a conclusão do carregamento do firmware, este será exibido na tabela Gerenciamento de firmware.
- 5 Na página Sistema > Configurações, clique no ícone Inicializar na linha de **Firmware transferido por upload – Novo!**
- 6 Na caixa de diálogo de confirmação, clique em **OK**. O dispositivo é reiniciado e a página de login é exibida.
- 7 Digite seu nome de usuário e sua senha. As informações da sua nova versão de imagem do SonicOS são exibidas na página Sistema > Status.

Atualizar firmware com as configurações padrão de fábrica

Para carregar firmware novo para seu dispositivo SonicWall e iniciá-lo usando as configurações padrão:

- 1 Baixe o arquivo de imagem de firmware do SonicOS a partir do MySonicWall e salve-o em seu computador local.
- 2 Direcione seu navegador para o endereço IP do dispositivo e efetue login como administrador.
- 3 Na página Sistema > Configurações, siga um dos seguintes procedimentos:

- Em um dispositivo SuperMassive ou NSA, clique em **Criar backup**.
- Em um dispositivo TZ ou SOHO W, clique em **Criar configurações de backup**.

Aguarde até o backup ser concluído.

- 4 Clique em **Carregar novo firmware**.
- 5 Navegue até o local onde salvou o arquivo de imagem de firmware do SonicOS, selecione o arquivo e clique em **Carregar**.
- 6 Na página Sistema > Configurações, clique no ícone Inicializar na linha de **Firmware transferido por upload com configurações padrão de fábrica – Novo!**
- 7 Na caixa de diálogo de confirmação, clique em **OK**. O dispositivo é reiniciado e, em seguida, exibe as opções para iniciar o Assistente de configuração ou ir para a página de login da interface de gerenciamento do SonicOS.

i **NOTA:** O endereço IP para a interface X0 (LAN) reverte para o padrão, 192.168.168.168. É possível efetuar logon no SonicOS conectando-se a X0 e direcionando o seu navegador para <https://192.168.168.168>. Em plataformas SonicWall NSA ou SuperMassive, também é possível efetuar logon conectando-se à porta MGMT e direcionando o seu navegador para <http://192.168.1.254>.

- 8 Insira o nome de usuário e a senha padrão (admin/password) para acessar a interface de gerenciamento do SonicOS.

Uso do Modo de segurança para atualizar o firmware

Se você não conseguir se conectar à interface de gerenciamento do SonicOS, poderá reiniciar o dispositivo de segurança SonicWall no Modo de segurança. O recurso Modo de segurança permite recuperar rapidamente de estados de configuração incertos com uma interface de gerenciamento simplificada que inclui as mesmas configurações disponíveis na página Sistema > Configurações.

Tópicos:

- [Uso do Modo de segurança na maioria das plataformas](#)
- [Uso do Modo de segurança no SuperMassive 9800](#)

Uso do Modo de segurança na maioria das plataformas

A implementação do Modo de segurança é compatível com as seguintes plataformas:

SuperMassive	NSA	TZ	SOHO
9200	2600	TZ300/TZ300W	SOHO W
9400	3600	TZ400/TZ400W	
9600	4600	TZ500/TZ500W	
	5600	TZ600	
	6600		

O procedimento de Modo de segurança usa um botão **Modo de segurança** embutido em um pequeno orifício próximo das portas USB na parte frontal do dispositivo SonicWall.

Para usar o Modo de segurança para atualizar o firmware em um dispositivo de segurança SonicWall:

- 1 Efetue uma das seguintes ações:
 - Em um dispositivo SonicWall TZ ou SOHO W, conecte seu computador à porta X0 no dispositivo e configure seu computador com um endereço IP na sub-rede 192.168.168.0/24, como 192.168.168.20.
 - Em um dispositivo SonicWall NSA ou SuperMassive, conecte seu computador à porta MGMT no dispositivo e configure seu computador com um endereço IP na sub-rede 192.168.1.0/24, como 192.168.1.20.
- 2 Use um objeto estreito e comprido, como um clipe esticado ou um palito, para pressionar e manter pressionado o botão Modo de segurança do dispositivo de segurança por mais de 20 segundos.
A luz de teste começa a piscar depois de o dispositivo ter reinicializado no Modo de segurança.
- 3 Execute um dos seguintes procedimentos para acessar a interface de gerenciamento do Modo de segurança:
 - Em um dispositivo SonicWall TZ ou SOHO W, aponte o navegador para <http://192.168.168.168>.
 - Em um dispositivo SonicWall NSA ou SuperMassive, aponte o navegador para <http://192.168.1.254>.
- 4 Clique em **Upload New Firmware (Carregar novo firmware)** e, em seguida, navegue até o local onde salvou a imagem de firmware do SonicOS, selecione o arquivo e clique em **Upload (Carregar)**.
- 5 Clique no ícone Inicializar na linha para realizar uma das seguintes opções:
 - **Uploaded Firmware – New! (Firmware transferido por upload – Novo!)**
Use esta opção para reiniciar o dispositivo com suas definições de configuração atuais.
 - **Uploaded Firmware with Factory Default Settings – New! (Firmware transferido por upload com configurações padrão de fábrica – Novo!)**
Use esta opção para reiniciar o dispositivo com as definições de configuração padrão de fábrica.
- 6 Na caixa de diálogo de confirmação, clique em **OK** para continuar.
- 7 Depois de uma reinicialização bem-sucedida do firmware, a tela de logon será exibida. Se reinicializou com configurações padrão de fábrica, insira o nome de usuário e a senha padrão (admin/senha) para acessar a interface de gerenciamento do SonicOS.

Em um dispositivo SonicWall NSA ou SuperMassive, é possível continuar gerenciando o dispositivo a partir da interface MGMT em 192.168.1.254.

Em todas as plataformas SonicWall, é possível gerenciar o dispositivo a partir da interface X0 ou outra interface LAN, bem como a partir da interface WAN, se configurada. O endereço IP padrão da interface X0 é 192.168.168.168.
- 8 Para gerenciar o dispositivo a partir de uma interface diferente daquela em que o computador esteja fisicamente conectado:
 - a Desconecte o seu computador do dispositivo.
 - b Reconfigure o computador para obter automaticamente um endereço IP e um endereço de servidor DNS ou redefina-o para seus valores estáticos normais.
 - c Conecte o computador à sua rede ou à interface desejada no dispositivo.
 - d Aponte seu navegador para o endereço IP adequado da WAN ou LAN do dispositivo.

Uso do Modo de segurança no SuperMassive 9800

A implementação do Modo de segurança é compatível com o SuperMassive 9800. Você pode ver as versões do ChassisOS e do FailSafe na interface do Modo de segurança.

Para usar o Modo de segurança para atualizar o firmware em um SuperMassive 9800:

- 1 Efetue login no dispositivo e navegue até a página Network > Interfaces (Rede > Interfaces).
- 2 Na tabela **Network Settings (Configurações de rede)**, clique no ícone Configurar da interface **MGMT**. A caixa de diálogo **Edit Interface – MGMT (Editar interface – MGMT)** é exibida.

The screenshot shows the 'Edit Interface – MGMT' configuration dialog box. It has two tabs: 'General' and 'Advanced'. The 'General' tab is selected. The title is 'Interface 'MGMT' Settings'. The fields are as follows:

Zone:	MGMT
IP Assignment:	Static IP Mode
IP Address:	10.206.22.102
Chassis IP Address:	10.206.22.101
Subnet Mask:	255.255.255.0
Default Gateway:	10.206.22.1
Comment:	Default MGMT
Management:	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> Ping <input type="checkbox"/> SNMP <input checked="" type="checkbox"/> SSH
User Login:	<input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> HTTPS
	<input type="checkbox"/> Add rule to enable redirect from HTTP to HTTPS
Chassis Management:	<input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> Ping <input type="checkbox"/> SNMP <input checked="" type="checkbox"/> SSH

- 3 Para o **Chassis Management (Gerenciamento de chassi)**, selecione as seguintes caixas de seleção:
 - HTTP
 - Ping
 - SSH
- 4 Clique em **OK**.

- 5 Direcione o seu navegador para o endereço IP do chassi, como `http://10.206.22.101` (utilize o endereço IP do chassi para a unidade primária em um par de HA). A página de Modo de segurança SonicOS é exibida.

Supermassive - SonicOS SafeMode
[Sign in\(SonicOS MGMT\)](#)







SonicOS SafeMode will allow you to:

- View current SonicOS, ChassisOS, and ROM versions.
- Upload SonicOS firmware images
- Boot SonicOS with current or factory default settings

System Information


Product name:	SuperMassive-E9800
Serial number:	COE-4E-454E-22
Authentication code:	R-4-X-22
ROM Chassis:	5.5.0.11
ROM Blade #1:	5.5.0.11
ROM Blade #2:	5.5.0.11
FailSafe:	6.2.1.7
ChassisOS:	6.0.3.5
ChassisOS Apps:	6.0.3.5
CPU type:	Cavium Octeon II V0.2
MemTotal:	2002180 kB

Firmware Management

Firmware Image	Version	Size	Download	Boot
Current Firmware	SonicOS Enhanced 6.2.1.3-56n	31.75 MiB		
Current Firmware with Factory Default Settings	SonicOS Enhanced 6.2.1.3-56n	31.75 MiB		
System Backup	SonicOS Enhanced 6.2.1.3-56n	31.75 MiB		

Upload New Firmware...

ChassisOS Management

ChassisOS Image	Version	Date	Install
Current Image	ChassisOS 6.0.3.5	MON APR 04 18:05:51 2016	

Upload New ChassisOS...

Status: Ready.

- 6 Clique em **Upload New Firmware (Carregar novo firmware)** e, em seguida, navegue até o local onde salvou a imagem de firmware do SonicOS, selecione o arquivo e clique em **Upload (Carregar)**.
- 7 Clique no ícone Inicializar na linha para realizar uma das seguintes opções:
- **Uploaded Firmware – New! (Firmware transferido por upload – Novo!)**
Use esta opção para reiniciar o dispositivo com suas definições de configuração atuais.

- **Uploaded Firmware with Factory Default Settings – New! (Firmware transferido por upload com configurações padrão de fábrica – Novo!)**

Use esta opção para reiniciar o dispositivo com as definições de configuração padrão de fábrica.

- 8 Na caixa de diálogo de confirmação, clique em **OK** para continuar.
- 9 Depois de uma reinicialização bem-sucedida do firmware, a tela de logon será exibida. Direcione o seu navegador para o endereço IP do dispositivo (não o endereço IP do chassi) e efetue logon ou utilize o endereço IP padrão caso tenha reinicializado com as configurações padrão de fábrica.

Se reinicializou com configurações padrão de fábrica, insira o nome de usuário e a senha padrão (admin/password) para acessar a interface de gerenciamento do SonicOS.

- 10 Navegue até a página Network > Interfaces (Rede > Interfaces).
- 11 Na tabela **Network Settings (Configurações de rede)**, clique no ícone Editar da interface **MGMT**.
- 12 Para o **Chassis Management (Gerenciamento de chassi)**, desmarque as seguintes caixas de seleção:
 - **HTTP**
 - **Ping**
 - **SSH**

Isto desabilita o recurso de Modo de segurança e protege o seu dispositivo de ser acessado sem autorização.

- 13 Clique em **OK**.

Sobre atualizações e túneis VPN

Foram implementadas alterações significativas de design para interfaces de túnel VPN no SonicOS 6.2.4, SonicOS 6.2.5 e novamente no SonicOS 6.2.6.

- O SonicOS 6.2.3 e versões anteriores são compatíveis com Interfaces de túnel não numeradas para roteamento estático e dinâmico (avançado), enquanto o SonicOS 6.2.4 somente é compatível com Interfaces de túnel numeradas, incluindo o suporte de roteamento avançado. Atualizar ou importar configurações de uma versão anterior para o SonicOS 6.2.4 pode implicar a reconfiguração manual das interfaces de túnel.
- O SonicOS 6.2.5 é compatível com Interfaces de túnel não numeradas e Interfaces de túnel numeradas em todas as plataformas. Atualizar a partir de todas as versões anteriores é totalmente compatível. Uma Interface de túnel não numerada é configurada criando uma política de VPN do tipo de política Interface de túnel e só pode ser usada com roteamento estático. Uma Interface de túnel numerada é configurada adicionando uma Interface de túnel VPN na página Rede > Interfaces e pode ser usada com roteamento estático ou dinâmico.
- O SonicOS 6.2.6 expande os recursos da versão 6.2.5 adicionando suporte de roteamento dinâmico (RIP, OSPF) em Interfaces de túnel não numeradas. O roteamento dinâmico é habilitado através da opção Permitir roteamento avançado na guia Avançado ao criar a política de VPN do tipo de política Interface de túnel.

Consulte o *Guia de administração do SonicOS 6.2* para obter mais informações.

Resumo da compatibilidade com interfaces de túnel no SonicOS:

Versão do firmware	Compatibilidade com interfaces de túnel
SonicOS 5.8.1/5.8.4	Compatível com Interfaces de túnel não numeradas em todas as plataformas.

SonicOS 5.9	Compatível apenas com Interfaces de túnel não numeradas nas séries TZ 105/200/205/210 e NSA 2400MX. A série TZ 100 não é compatível com roteamento dinâmico (não tem Roteamento avançado) em Interfaces de túnel não numeradas. Compatível com Interfaces de túnel numeradas e com interfaces de túnel não numeradas nas restantes plataformas (série TZ 215, NSA, E-Class NSA).
SonicOS 6.1	Compatível com Interfaces de túnel não numeradas em todas as plataformas.
SonicOS 6.2 até 6.2.2.2 e 6.2.3.1	Compatível com Interfaces de túnel não numeradas em todas as plataformas.
SonicOS 6.2.4	Compatível com Interfaces de túnel numeradas em todas as plataformas.
SonicOS 6.2.5	Compatível com Interfaces de túnel não numeradas e Interfaces de túnel numeradas em todas as plataformas. Apenas as Interfaces de túnel numeradas suportam roteamento dinâmico.
SonicOS 6.2.6	Compatível com Interfaces de túnel não numeradas e Interfaces de túnel numeradas em todas as plataformas. Tanto as Interfaces de túnel não numeradas como as numeradas suportam roteamento dinâmico e estático.

Em interfaces de túnel numeradas, as alterações no SonicOS 6.2.4.2 e 6.2.5.1 podem causar uma incompatibilidade na MTU (unidade máxima de transmissão) do OSPF nas seguintes situações:

- Um túnel usando criptografia que não AES é alterado para AES após a atualização do firewall de uma versão anterior para a versão 6.2.5.1 ou posterior.
- Existe um túnel usando criptografia AES entre dois firewalls com versões anteriores e somente um firewall é atualizado para a versão 6.2.5.1 ou posterior.
- Em um firewall com a versão 6.2.4.2 ou posterior, a MTU é alterada na interface que termina um túnel de VPN, fazendo com que a MTU da interface de túnel numerada se altere.

Aconselha-se aos administradores verificar a configuração de MTU em ambos os pontos terminais de troca de tráfego de VPN para assegurar que os valores correspondam e o OSPF possa estabelecer adjacência vizinha.

Consulte o artigo da Base de conhecimentos SW10735 para obter mais informações sobre o OSPF e interfaces de túnel, disponível em: <https://support.sonicwall.com/pt-br/sonicwall-tz-series/kb/sw10735>

Importar as definições de configuração

Você pode importar definições de configuração de um dispositivo para outro, o que pode poupar muito tempo durante a substituição de um dispositivo mais antigo por um novo modelo. Esta funcionalidade também é útil quando você precisa de vários dispositivos com definições de configuração semelhantes.

A importação de definições de configuração, ou preferências ("prefs."), para dispositivos de segurança de rede SonicWall funcionando com o SonicOS 6.2 é normalmente compatível com os seguintes dispositivos SonicWall funcionando com as versões 5.8, 5.9, 6.1 ou 6.2:

- SuperMassive 9600/9400/9200 (Gen 6)
- NSA 6600/5600/4600/3600/2600 (Gen 6)
- TZ600, TZ500/TZ500 W, TZ400/TZ400 W, TZ300/TZ300 W e SOHO/SOHO W (Gen 6)
- NSA E8510/E8500/E7500/E6500/E5500 (Gen 5)

- NSA 5000/4500/3500/2400, NSA 250M/250MW e NSA 220/220W (Gen 5)
- Séries TZ 215/210/205/200/105/100 (Gen 5)

i **IMPORTANTE:** Consulte [Sobre atualizações e túneis VPN](#) para obter informações sobre alterações de design em interfaces de túnel VPN no SonicOS 6.2.4, 6.2.5 e 6.2.6.

A importação das definições de configuração para um SuperMassive 9800 com o SonicOS 6.2.1.x é suportada nos seguintes dispositivos com o SonicOS 6.2.0.x:

- SuperMassive 9600/9400/9200
- NSA 6600/5600/4600/3600/2600

i **NOTA:** A importação de configurações para um SuperMassive 9800 de aplicativos com versões do SonicOS diferentes de 6.2.0.x ou 6.2.1.x não é compatível.

Para exportar as definições de configuração de um dispositivo, navegue até a página Sistema > Configurações no SonicOS e clique no botão Exportar configurações. Você pode então importar o arquivo de configurações para outro dispositivo clicando no botão Importar configurações nessa página.

As tabelas nas seções seguintes fornecem detalhes sobre quais versões de firmware ou quais modelos são compatíveis com a importação de definições de configuração para outros modelos e outras versões de firmware para 5.8, 5.9, 6.1 ou 6.2.

Consulte as seções a seguir:

- [Versões do SonicOS compatíveis com importação de definições de configuração](#)
- [Tabelas de compatibilidade de importação de configurações de plataforma](#)

Versões do SonicOS compatíveis com importação de definições de configuração

A seguinte tabela ilustra as versões de origem e destino do SonicOS compatíveis com importação de definições de configuração de um dispositivo para outro.

Apoio de importação/exportação de configurações para o SonicOS

	Para					
		5.8 (Min. 5.8.1.12)	5.9	6.1.1.x	6.1.2.x	6.2
De	5.8 (Min. 5.8.1.12)	Y	Y	Y	Y	Y
	5.9	N	Y	N	N	Y (Min. 5.9.0.4)
	6.1.1.x	N	N	Y	Y	Y
	6.1.2.x	N	N	Y	Y	Y
	6.2	N	N	N	N	Y

Se a resposta acima for "Y", consulte a tabela abaixo para seus produtos específicos

Se a resposta acima for "N", esta atualização de configurações não é suportada

Tabelas de compatibilidade de importação de configurações de plataforma

As tabelas nas seguintes seções mostram os firewalls da SonicWall cujas definições de configuração podem ser importadas para plataformas SonicWall Gen 6 com SonicOS 6.2. Os firewalls de origem estão listados na coluna esquerda e os firewalls de destino estão listados no topo.

A legenda para essas tabelas é:

Y	Suportado
N	Não suportado. Embora a importação do arquivo de configurações possa ser bem-sucedida, as limitações do firewall poderão resultar na remoção de itens como escopos DHCP, configurações de VPN, etc.
C	Informações de configuração de interfaces extras serão removidas. As políticas de NAT, regras de acesso do firewall e outras configurações dependentes de interface também serão removidas.

Consulte as seções a seguir:

- [Compatibilidade de importação de configurações TZ/SOHO W](#)
- [Compatibilidade de importação de configurações NSA/SuperMassive](#)

Compatibilidade de importação de configurações TZ/SOHO W

FIREWALLS DE DESTINO

	SOHO W	TZ300	TZ300W	TZ400	TZ400W	TZ500	TZ500W	TZ600	
F	SOHO	C	Y	C	Y	C	Y	C	Y
I	SOHO W	Y	C	Y	C	Y	C	Y	C
R	TZ 100 / TZ 200	Y	Y	Y	Y	Y	Y	Y	Y
E	TZ 100W / TZ 200W	Y	C	Y	C	Y	C	Y	C
W	TZ 105 / TZ 205	Y	Y	Y	Y	Y	Y	Y	Y
A	TZ 105W / TZ 205W	Y	C	Y	C	Y	C	Y	C
L	TZ 210	C	C	C	Y	Y	Y	Y	Y
L	TZ 210W	C	C	C	C	Y	C	Y	C
S	TZ 215	C	C	C	Y	Y	Y	Y	Y
	TZ 215W	C	C	C	C	Y	C	Y	C
D	TZ300	Y	Y	Y	Y	Y	Y	Y	Y
E	TZ300W	Y	C	Y	C	Y	C	Y	C
	TZ400	C	C	C	Y	Y	Y	Y	Y
O	TZ400W	C	C	C	C	Y	C	Y	C
R	TZ500	C	C	C	C	C	Y	Y	Y
I	TZ500W	C	C	C	C	C	C	Y	C
G	TZ600	C	C	C	C	C	C	C	Y
E	NSA 220	C	C	C	Y	Y	Y	Y	Y
M	NSA 220W	C	C	C	C	Y	C	Y	C
	NSA 240	C	C	C	C	C	C	C	Y
	NSA 250M	N	N	N	N	N	Y	Y	Y
	NSA 250MW	N	N	N	N	N	C	Y	C
	NSA 2400	N	N	N	N	N	N	N	Y
	NSA 2400MX	N	N	N	N	N	N	N	C
	NSA 3500	N	N	N	N	N	N	N	N
	NSA 4500	N	N	N	N	N	N	N	N
	NSA 5000	N	N	N	N	N	N	N	N
	NSA E5500	N	N	N	N	N	N	N	N
	NSA E6500	N	N	N	N	N	N	N	N
	NSA E7500	N	N	N	N	N	N	N	N
	NSA E8500	N	N	N	N	N	N	N	N
	NSA E8510	N	N	N	N	N	N	N	N
	NSA 2600	N	N	N	N	N	N	N	N
	NSA 3600	N	N	N	N	N	N	N	N
	NSA 4600	N	N	N	N	N	N	N	N
	NSA 5600	N	N	N	N	N	N	N	N
	NSA 6600	N	N	N	N	N	N	N	N
	SM 9200	N	N	N	N	N	N	N	N
	SM 9400	N	N	N	N	N	N	N	N
	SM 9600	N	N	N	N	N	N	N	N
	SM 9800	N	N	N	N	N	N	N	N

Compatibilidade de importação de configurações NSA/SuperMassive

FIREWALLS DE DESTINO

		NSA 2600	NSA 3600	NSA 4600	NSA 5600	NSA 6600	SM 9200	SM 9400	SM 9600	SM 9800
F	SOHO	N	N	N	N	N	N	N	N	N
	SOHO W	N	N	N	N	N	N	N	N	N
I	TZ 100 / TZ 200	N	N	N	N	N	N	N	N	N
	TZ 100W / TZ 200W	N	N	N	N	N	N	N	N	N
R	TZ 105 / TZ 205	N	N	N	N	N	N	N	N	N
	TZ 105W / TZ 205W	N	N	N	N	N	N	N	N	N
E	TZ 210	N	N	N	N	N	N	N	N	N
	TZ 210W	N	N	N	N	N	N	N	N	N
W	TZ 215	N	N	N	N	N	N	N	N	N
	TZ 215W	N	N	N	N	N	N	N	N	N
A	TZ300	N	N	N	N	N	N	N	N	N
	TZ300W	N	N	N	N	N	N	N	N	N
L	TZ400	N	N	N	N	N	N	N	N	N
	TZ400W	N	N	N	N	N	N	N	N	N
S	TZ500	Y	Y	Y	Y	Y	Y	Y	Y	N
	TZ500W	C	C	C	C	C	C	C	C	N
D	TZ600	Y	Y	Y	Y	Y	Y	Y	Y	N
	NSA 220	Y	Y	Y	Y	Y	Y	Y	Y	N
E	NSA 220W	N	N	N	N	N	N	N	N	N
	NSA 240	C	Y	Y	Y	Y	Y	Y	Y	N
O	NSA 250M	N	N	N	N	N	N	N	N	N
	NSA 250MW	N	N	N	N	N	N	N	N	N
R	NSA 2400	Y	Y	Y	Y	Y	Y	Y	Y	N
	NSA 2400MX	N	N	N	N	N	N	N	N	N
I	NSA 3500	Y	Y	Y	Y	Y	Y	Y	Y	N
	NSA 4500	Y	Y	Y	Y	Y	Y	Y	Y	N
G	NSA 5000	Y	Y	Y	Y	Y	Y	Y	Y	N
	NSA E5500	N	Y	Y	Y	Y	Y	Y	Y	N
E	NSA E6500	N	Y	Y	Y	Y	Y	Y	Y	N
	NSA E7500	N	Y	Y	Y	Y	Y	Y	Y	N
M	NSA E8500	N	Y	Y	Y	Y	Y	Y	Y	N
	NSA E8510	N	Y	Y	Y	Y	Y	Y	Y	N
	NSA 2600	Y	Y	Y	Y	Y	Y	Y	Y	N
	NSA 3600	N	Y	Y	Y	Y	Y	Y	Y	N
	NSA 4600	N	Y	Y	Y	Y	Y	Y	Y	N
	NSA 5600	N	Y	Y	Y	Y	Y	Y	Y	N
	NSA 6600	N	Y	Y	Y	Y	Y	Y	Y	N
	SM 9200	Y	Y	Y	Y	Y	Y	Y	Y	N
	SM 9400	Y	Y	Y	Y	Y	Y	Y	Y	N
	SM 9600	Y	Y	Y	Y	Y	Y	Y	Y	N
	SM 9800	N	N	N	N	N	N	N	N	Y

Suporte da SonicWall

O suporte técnico está disponível para clientes que tiverem comprado produtos da SonicWall com um contrato de suporte de manutenção válido e para clientes com versões de avaliação.

O Portal de suporte fornece ferramentas de autoajuda que você pode usar para solucionar problemas com rapidez e de forma independente, 24 horas por dia, 365 dias por ano. Acesse o Portal de suporte em <https://support.sonicwall.com/pt-br/>.

O Portal de suporte permite:

- Visualizar artigos da base de conhecimentos e documentação técnica
- Baixar software
- Visualizar tutoriais em vídeo
- Colaborar com pares e especialistas em fóruns de usuários
- Obter assistência sobre licenciamento
- Acessar MySonicWall
- Conhecer os serviços profissionais SonicWall
- Registrar-se em treinamentos e certificação

Para entrar em contato com o suporte da SonicWall, visite <https://support.sonicwall.com/pt-br/contact-support>.

Copyright © 2017 SonicWall Inc. Todos os direitos reservados.

Este produto está protegido por leis de propriedade intelectual e direitos autorais dos EUA e internacionais. SonicWall é uma marca comercial ou marca comercial registrada da SonicWall Inc. e/ou respectivos afiliados nos EUA e/ou em outros países. Todas as outras marcas comerciais registradas são propriedade dos respectivos proprietários.

As informações neste documento são fornecidas em conexão com os produtos da SonicWall Inc. e/ou respectivos afiliados. Nenhuma licença, explícita ou implícita, por preclusão ou de outra forma, para qualquer direito de propriedade intelectual é concedida por este documento ou em conexão com as vendas de produtos SonicWall. EXCETO CONFORME DISPOSTO NOS TERMOS E CONDIÇÕES, COMO ESPECIFICADO NO CONTRATO DE LICENÇA PARA ESTE PRODUTO, A SONICWALL E/OU RESPECTIVOS AFILIADOS NÃO ASSUMEM QUALQUER RESPONSABILIDADE E NEGAM QUALQUER GARANTIA, EXPRESSA, IMPLÍCITA OU LEGAL RELACIONADA A SEUS PRODUTOS INCLUINDO, MAS NÃO LIMITANDO, A GARANTIA IMPLÍCITA DE COMERCIALIZAÇÃO, ADAPTAÇÃO PARA UMA DETERMINADA FINALIDADE OU NÃO INFRAÇÃO. EM NENHUMA CIRCUNSTÂNCIA A SONICWALL E/OU RESPECTIVOS AFILIADOS DEVEM SER CONSIDERADOS RESPONSÁVEIS POR QUALQUER DANO DIRETO, INDIRETO, EVENTUAL, PUNITIVO, ESPECIAL OU INCIDENTAL (INCLUINDO, SEM LIMITAÇÕES, DANOS POR PERDAS DE LUCROS, INTERRUPTÃO DO TRABALHO OU PERDA DE INFORMAÇÕES) DEVIDO AO USO OU INCAPACIDADE DE USO DESTE DOCUMENTO, MESMO QUE A SONICWALL E/OU RESPECTIVOS AFILIADOS TENHAM SIDO ALERTADOS QUANTO À POSSIBILIDADE DE TAIS DANOS. A SonicWall e/ou respectivos afiliados não garantem as representações ou fazem garantias no que diz respeito à precisão e integridade dos conteúdos deste documento e reservam o direito a alterar as especificações e descrições dos produtos a qualquer momento sem aviso prévio. A SonicWall Inc. e/ou respectivos afiliados não estabelecem nenhum compromisso para a atualização das informações contidas neste documento.

Para obter mais informações, visite <https://www.sonicwall.com/br-pt/legal/>.

Legenda



AVISO: O ícone AVISO indica risco de danos ao equipamento, ferimentos ou morte.



CUIDADO: O ícone CUIDADO indica um possível dano ao hardware ou perda de dados se as instruções não forem seguidas.



IMPORTANTE, NOTA, DICA, DISPOSITIVOS MÓVEIS ou VÍDEO: Um ícone de informação que indica informações de suporte.