# Manual de Reinstalação do Sistema Operacional GAIA Através de Pen Drive Bootável no Firewall Check Point

1. Para reinstalar o Sistema Operacional GAIA do Check Point através de um pen drive Bootável é necessário primeiro preparar o pen drive para que ele se torne Bootável. Dado isso, execute o programa ISOMorphic como administrador:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Após abrir o ISOMorphic informe a imagem ISO do GAIA Check Point R77.30 Gaia disponibilizada pelo professor Paulo Santanna e informe o pen drive que será formatado:

**(Check\_Point\_R77.30\_3000\_5000\_15000\_23000\_Sabdblast\_Appliances\_T22.iso)**

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Haverá uma tela de confirmação onde você deve digitar a palavra “yes” no campo em branco e clicar em *yes,* confirmando assim que está ciente de que o pen drive será formatado:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Aguarde enquanto o processo de formatação do pen drive está em andamento:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Ao concluir, o pen drive pode ser ejetado:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Conecte o pen drive no Firewall Check Point:



1. Execute o “putty” para ter acesso ao terminal:

Uma imagem contendo captura de tela

Descrição gerada com alta confiança

1. Conecte um cabo console e um teclado USB no Check Point:



1. E no Computador Administrador do Check Point:



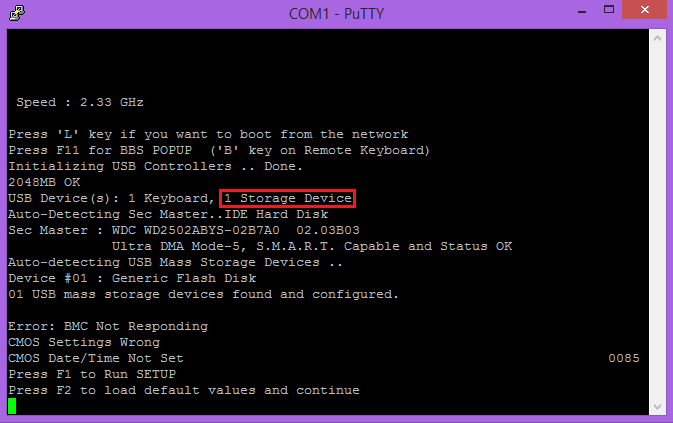
1. Selecione tipo de conexão *Serial* e mude a velocidade para *19200*:

***Obs.:*** Caso ocorra algum problema com o acesso ao Check Point ou algo incomum na inicialização tente novamente com a velocidade em 9600.

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Note que ao iniciar ele informa que foi detectado um dispositivo USB, após certificar que o pen drive foi reconhecido aperte F1:



1. Ao aparecer a tela de senha da ROM, já que não temos a senha da ROM, de *Enter* 3 vezes que irá pular para a próxima tela:

Uma imagem contendo captura de tela, equipamentos eletrônicos

Descrição gerada com muito alta confiança

1. Chegando a tela desejada ira perguntar de qual maneira deseja dar boot, use a tecla *<tab>* para ver as opções, e digite “serial”

Uma imagem contendo captura de tela, equipamentos eletrônicos

Descrição gerada com muito alta confiança

1. Será informado o carregamento do dispositivo USB:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Após o dispositivo ser carregado com sucesso informará o começo do processo de reinstalação do GAIA no Check Point

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

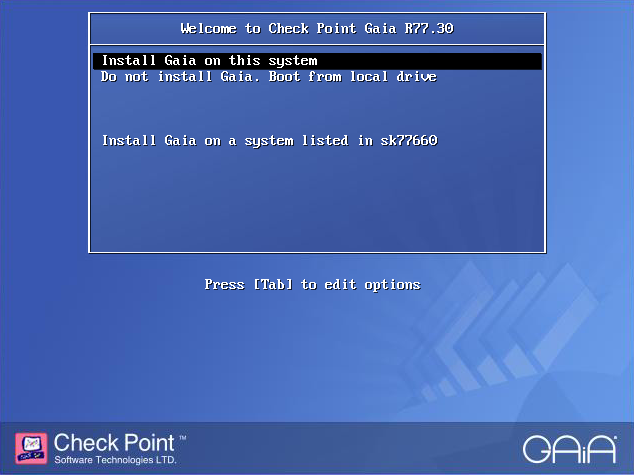
1. Por fim, aguarde até que o processo seja finalizado e o firewall reinicializado. Portanto o Firewall Check Point já está com o Sistema Operacional GAIA reinstalado.

# Manual de Instalação e Configuração do Firewall Check Point

1. Para instalar o Check Point é necessário a instalação do Gaia, o OS único da Check Point para aplicações de segurança. Assim sendo de boot utilizando a imagem ISO Check Point R77.30 Gaia disponibilizada pelo professor Paulo Sant’Anna:

**(Check\_Point\_R77.30\_3000\_5000\_15000\_23000\_Sabdblast\_Appliances\_T22.iso)**

***Obs.:*** É necessário um armazenamento mínimo de 100 GB para um funcionamento considerável.



1. Após a tela de boas-vindas, selecione o idioma do teclado:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Configure as partições do disco:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Atribua uma senha para o usuário admin:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Atribua IP a interface eth0:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Ao finalizar o processo de instalação do OS Gaia, terá um aviso alertando como acessar o Check Point via interface web:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Use um cliente para testar a conexão entre eles:

Uma imagem contendo captura de tela, equipamentos eletrônicos, monitor

Descrição gerada com muito alta confiança

1. Abra o browser e na barra de endereços coloque o ip do Check Point, note que ele utiliza o protocolo https:

***Obs.:*** Ocorreram alguns problemas de certificados no Chrome portanto foi utilizado o Internet Explorer para acesso via interface web.

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Faça o Login com o usuário admin:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Por ser a primeira vez que estará utilizando o Check Point, abrirá o assistente de Configurações do Check Point:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Mantenha a interface já configurada

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Se desejar, altere o nome do Firewall:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Acerte a data e hora do Check Point

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Selecione o tipo de instalação:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Deixe as opções selecionadas por padrão e prossiga:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Configure entre quem terá acesso a interface web do Check Point, se qualquer IP poderá fazer uma requisição web, uma rede, um range ou apenas a maquina atual:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Finalize a instalação e aguarde enquanto as alterações são aplicadas:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Uma vez dentro da interface web, o computador administrador necessita de um assistente para fazer as aplicações do Firewall Check Point, o SmartConsole. Faça o download como exibido na imagem abaixo:

Uma imagem contendo captura de tela

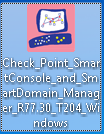
Descrição gerada com muito alta confiança

1. Após o download extraia os arquivos e execute o arquivo setup. Siga as etapas repetitivas de Next na instalação e instale o SmartConsole:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. A etapa a seguir é caso ocorra algum erro durante a instalação do SmartConsole exibida acima. Em alguns casos o SmartConsole não era instalado com sucesso, se isso acontecer, desinstale e exclua tudo relativo ao SmartConsole e utilize o executável disponibilizado pelo professor Paulo Santanna para instalá-lo:



1. Depois de instalado, conecte-se através SmartDashboard para começar a fazer aplicações no Firewall:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Para criar uma regra, na aba “Policy”, clique no ícone em destaque:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Para editar um campo, clique com o botão direito encima do campo que deseja editar e selecione “Edit...” como no exemplo abaixo para alterar o nome de regra:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. É necessário definir a sua LAN manualmente, para isso clique com o botão direito em “Networks” e “Network...”, após informe o nome e IP da rede:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. O Ping é recusado por padrão, portanto, a Rede Local não consegue estabelecer uma conexão Ping para fazer alguns testes, como exemplo crie uma regra para permitir Ping da LAN para o Check Point:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Para que as regras criadas sejam aplicadas definitivamente, é preciso salvar e selecionar “Install Policy”:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Abaixo exibe uma imagem de um host da Rede Local tentando estabelecer o Ping antes da etapa do “Install Policy” e após as regras serem aplicadas. Sendo assim foi possível haver uma conexão entre eles:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Regra de bloqueio de SSH como exemplo, certo host apesar de estar na Rede Local, não deve conseguir estabelecer conexão SSH com o Check Point, por tanto foi feita uma regra onde se aquele host em específico tentar fazer um acesso SSH com o Check Point essa solicitação deve ser negada:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Antes de ser aplicada a regra acima, este host por ser um host da Rede Local tinha acesso SSH com o Check Point:

Uma imagem contendo captura de tela, equipamentos eletrônicos

Descrição gerada com muito alta confiança

1. Após ter sido aplicada a regra o mesmo host tenta acessar o Check Point pelo protocolo SSH e como resultado é negado:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Para habilitar acesso a internet para os clientes através de NAT, é necessário criar uma regra:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. O Firewall Check Point precisa de outra interface que tenha acesso a internet, para isso, na interface web, foi configurado a “eth1” em DHCP, para que ela consiga se comunicar com a Rede WAN:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Ainda na interface web, na aba “IPv4 Static Routes”, deve ser apontado o gateway da interface WAN, que no caso é o gateway da interface eth1:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Por fim, vá até a interface LAN criada nas etapas anteriores e edite-a, na aba “NAT”, marque a opção “Add Automatic Address Translation rules”:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Pelo fato de não ter um DNS configurado na rede para a resolução de nomes, foi configurado manualmente o DNS no cliente:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. A imagem a seguir mostra um cliente tentando acessar a pagina do MSN antes de serem realizadas todas as configurações anteriores:

Uma imagem contendo captura de tela

Descrição gerada com muito alta confiança

1. Depois de serem realizadas as configurações citadas anteriormente o cliente tenta acessar a pagina do MSN e este é o resultado:

