CONTENTS

RELATED

Como configurar as chaves SSH no CentOS

View

Como usar o nsh para executar comandos remotos seguros no Ubuntu 18.04

View

// Tutorial //

7 Medidas de Segurança para Proteger Seus Servidores

Published on March 8, 2018

Security Firewall Conceptual Networking VPN

By Justin Ellingwood

Developer and author at DigitalOcean.

Introdução

Ao configurar a infraestrutura, colocar suas aplicações para funcionar será por muitas vezes a sua primeira preocupação. Contudo, colocar suas aplicações para funcionar corretamente sem atender às necessidades de segurança de sua infraestrutura pode ter consequências devastadoras no futuro.

Neste guia, iremos falar sobre algumas práticas básicas de segurança que são melhor configuradas antes ou enquanto você configura suas aplicações.

Chaves SSH

Chaves SSH é um par de chaves criptográficas que podem ser utilizadas para se autenticar em um servidor SSH como uma alternativa aos logins baseados em senha. Um par de chaves privada e pública são criados antes da autenticação. A chave privada é mantida em segredo e segura pelo usuário, enquanto a chave pública pode ser compartilhada com qualquer um.

Para configurar a autenticação por chave SSH, você deve colocar a chave pública do usuário no servidor em um diretório especial. Quando o usuário se conecta ao servidor, o servidor irá solicitar provas de que o cliente possui a chave privada associada. O cliente SSH irá utilizar a chave privada para responder de uma forma que comprova a propriedade da mesma. O servidor então irá deixar o cliente se conectar sem uma senha. Para aprender mais sobre como funcionam as chaves SSH, veja nosso artigo aqui.

Como Elas Melhoram a segurança?

Com o SSH, qualquer tipo de autenticação, incluindo a autenticação por senha, é completamente criptografada. Contudo, quando logins baseados em senha são permitidos, usuários maliciosos podem tentar repetidamente acessar o servidor. Com a força da computação moderna, é possível ganhar a entrada em um servidor automatizando essas tentativas e tentando, combinação por combinação, até que a senha correta seja encontrada.

A configuração da autenticação por chave SSH o permite desativar a autenticação baseada em senha. Chaves SSH geralmente possuem muito mais bits de dados do que uma senha, o que significa que há significativamente mais combinações possíveis que um atacante teria que executar. Muitos algoritmos de chave SSH são considerados inquebráveis pelo hardware de computação moderna, simplesmente porque exigiriam muito tempo para executar as possíveis correspondências.

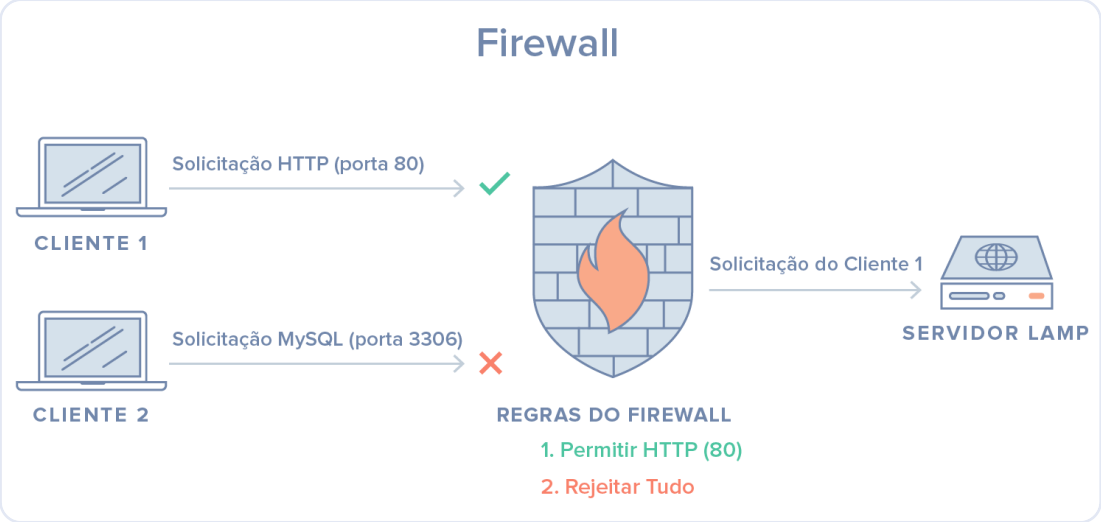
Quão difícil é implementar isto?

Chaves SSH são muito fáceis de configurar e é a maneira recomendada de fazer login em qualquer ambiente de servidor Linux ou Unix remotamente. Um par de chaves SSH pode ser gerado em sua máquina e você pode transferir a chave pública para seus servidores em poucos minutos.

Para aprender como configurar as chaves, siga este guia. Se você ainda sente que precisa da autenticação por senha, considere a implementação de uma solução como o fail2ban em seus servidores para limitar suposições de senhas.

Firewalls

Um firewall é uma peça de software (ou hardware) que controla quais serviços são expostos para a rede. Isto significa o bloqueio ou restrição de acesso a todas as portas exceto para aquelas que devem estar publicamente disponíveis.



Em um servidor típico, um número de serviços podem estar em execução por padrão. Estes podem ser categorizados nos seguintes grupos:

- Serviços públicos que podem ser acessados por qualquer pessoa na internet, geralmente anonimamente. Um bom exemplo disso é um servidor web que pode permitir o acesso ao seu site.
- Serviços privados que devem ser acessados somente por um grupo selecionado de contas autorizadas ou a partir de certos locais. Um exemplo disso pode ser um painel de controle de um banco de dados.
- Serviços internos que devem estar acessíveis somente a partir do próprio servidor, sem expor o serviço ao mundo exterior. Por exemplo, poderia ser um banco de dados que somente aceita conexões locais.

Firewalls podem assegurar que o acesso ao seu software está restrito de acordo com as categorias acima. Serviços públicos podem ser deixados abertos e disponíveis para todos e os serviços privados podem ser restringidos baseado em diferentes critérios. Serviços internos podem ser completamente inacessíveis ao mundo exterior. Para portas que não estão sendo utilizadas, o acesso é bloqueado completamente na maioria das configurações.

Como Eles Melhoram a Segurança?

Firewalls são uma parte essencial de qualquer configuração de servidor. Mesmo se seus serviços por si mesmos implementem funcionalidades de segurança ou estão restritos às interfaces nas quais você deseja que eles sejam executados, um firewall serve como uma camada extra de proteção.

Um firewall configurado apropriadamente irá restringir o acesso a tudo, exceto os serviços específicos que você precisa manter abertos. A exposição de apenas algumas peças de software reduz a superfície de ataque do seu servidor, limitando os componentes que são vulneráveis à exploração.

Quão difícil é implementar isto?

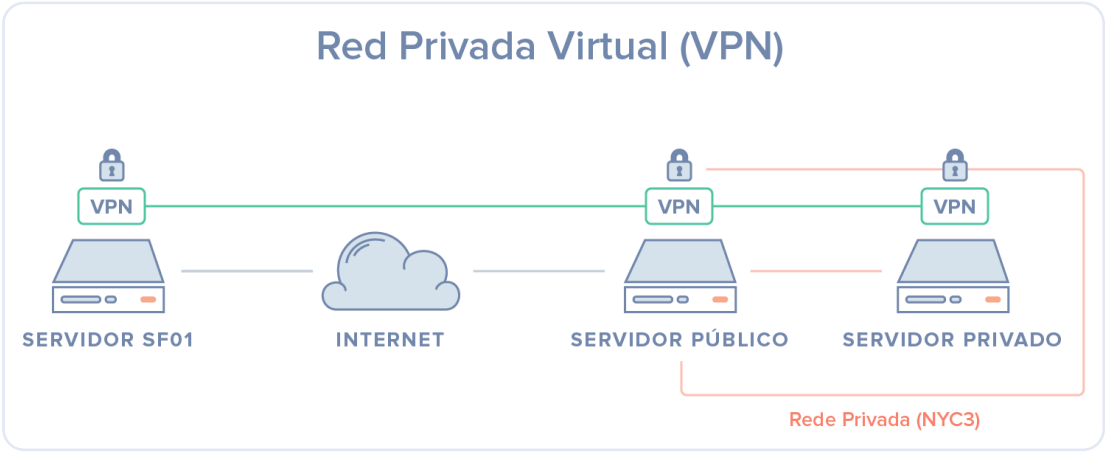
Existem muitos firewalls disponíveis para sistemas Linux, alguns dos quais têm uma curva de aprendizado mais acentuada do que outros. Em geral, no entanto, configurar um firewall deve tomar apenas poucos minutos e só precisa acontecer durante a configuração inicial do seu servidor ou quando você faz alterações nos serviços oferecidos no seu computador.

Um escolha simples é o UFW firewall. Outra opção é utilizar o iptables ou o CSF firewall.

VPNs e Redes Privadas

Redes privadas são redes que estão disponíveis somente para certos servidores ou usuários. Por exemplo, na DigitalOcean, a rede privada está disponível em algumas regiões como uma rede ampla de data center.

Uma VPN, ou Rede Virtual Privada, é uma forma de criar conexões seguras entre computadores remotos e apresentar a conexão como se fosse uma rede privada local. Isto fornece uma forma de configurar seus serviços como se eles estivessem em uma rede privada e conectar servidores remotos em cima de conexões seguras.



Como Elas Melhoram a Segurança?

A utilização de rede privada em vez de rede pública para comunicações internas é quase sempre preferível dada a escolha entre os dois. Contudo, uma vez que outros usuários dentro do data center podem acessar a mesma rede, você ainda deve implementar medidas adicionais para proteger a comunicação entre seus servidores.

A utilização de uma VPN é, efetivamente, uma maneira de mapear uma rede privada que apenas seus servidores podem ver. A comunicação será completamente privada e segura. Outras aplicações podem ser configuradas para repassar seu tráfego através da interface virtual que o software de VPN expõe. Desta forma, apenas os serviços que se destinam a serem consumidos pelos clientes na internet pública precisam ser expostos na rede pública.

Quão difícil é implementar isto?

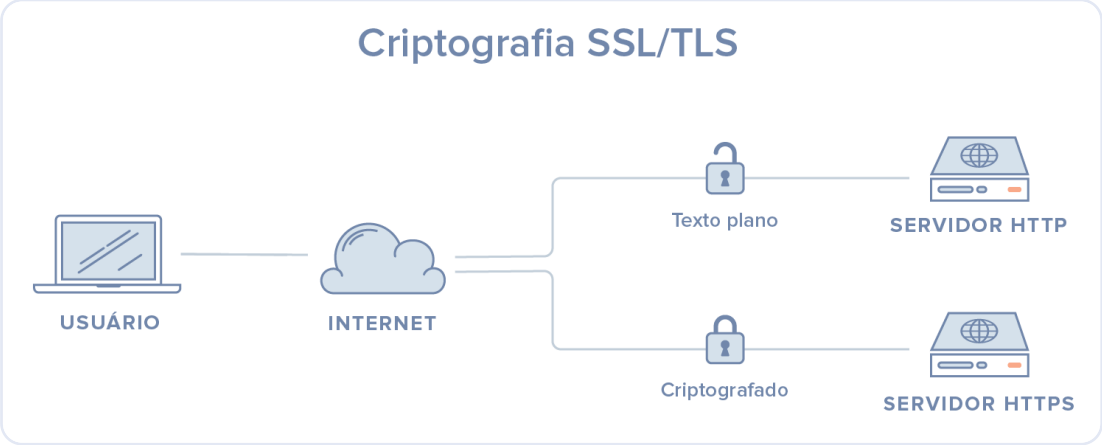
A utilização de redes privadas em um datacenter que tem essa capacidade é simples como ativar a

A utilização de redes privadas em um datacenter que tem essa capacidade é simples como ativar a interface durante a criação de seu servidor e configurar suas aplicações e o firewall para utilizar a rede privada. Tenha em mente que as redes privadas amplas de datacenter compartilham espaço com outros servidores que utilizam a mesma rede.

Quanto à VPN, a configuração inicial é um pouco mais trabalhosa, mas a segurança aumentada vale à pena para a maioria dos casos de uso. Cada servidor em uma VPN deve ter a segurança compartilhada e dados de configuração necessários para estabelecer a conexão segura instalada e configurada. Depois que a VPN estiver funcionando, aplicações devem ser configuradas para utilizar o túnel VPN. Para aprender sobre como configurar uma VPN para conectar com segurança a sua infraestrutura, veja nosso tutorial OpenVPN.

Infraestrutura de Chave Pública e Criptografia SSL/TLS

Infraestrutura de chave pública, ou PKI, refere-se a um sistema que é projetado para criar, gerenciar, e validar certificados para identificação de indivíduos e criptografia de comunicação. Certificados SSL ou TLS podem ser utilizados para autenticar diferentes entidades entre si. Após a autenticação, eles podem também ser utilizados para criptografar a comunicação.



Como Ela Melhora a Segurança?

Estabelecer uma autoridade de certificação e gerenciar certificados para seus servidores permite que cada entidade dentro de sua infraestrutura valide a identidade dos outros membros e criptografe seu tráfego. Isto pode prevenir ataques de man-in-the-middle onde um atacante imita um servidor em sua infraestrutura para interceptar tráfego.

Cada servidor pode ser configurado para confiar em uma autoridade de certificação centralizada. Posteriormente, qualquer certificado que a autoridade assinar pode ser implicitamente confiável. Se as aplicações e protocolos que você utiliza para comunicação suportam criptografia SSL/TLS, esta é uma forma de criptografar seu sistema sem a sobrecarga de um túnel VPN (que também muitas vezes usa SSL internamente).

Quão difícil é implementar isto?

A configuração de uma autoridade certificadora e o ajuste do restante da infraestrutura de chave pública pode envolver um pouco de esforço inicial. Além disso, a administração de certificados pode criar uma carga administrativa adicional quando novos certificados precisam ser criados, assinados, ou revogados.

Para muitos usuários, a implantação de uma infraestrutura de chave pública plena fará mais sentido à medida que sua infraestrutura precisar crescer. A proteção das comunicações entre os componentes utilizando VPN pode ser uma boa medida paliativa até que você chegue a ponto onde os custos da administração da PKI valham à pena.

Auditoria do Serviço

Até este ponto, temos discutido algumas tecnologias que você pode implementar para melhorar sua segurança. Contudo, uma grande parte da segurança está na análise de seus sistemas, entendendo as superfícies de ataque disponíveis, e bloqueando os componentes o melhor que puder.

A auditoria de serviço é um processo de descoberta de quais serviços estão rodando nos servidores da sua infraestrutura. Frequentemente, o sistema operacional padrão é configurado para executar certos serviços na inicialização. A instalação de software adicional pode, às vezes, criar dependências que também são iniciadas automaticamente.

A auditoria de serviço é uma forma de saber quais serviços estão em execução em seus sistemas, que portas eles estão utilizando para comunicação, e quais protocolos são aceitos. Esta informação pode ajudá-lo a configurar os ajustes do seu firewall.

Como Ela Melhora a Segurança?

Os servidores iniciam muitos processos para propósitos internos e para lidar com clientes externos. Cada um destes representam uma superfície expandida de ataque para usuários maliciosos. Quanto mais serviços você tiver executando, maior a chance há de que uma vulnerabilidade exista em seu software acessível.

Uma vez que você tenha ideia de quais serviços de rede estão executando em sua máquina, você pode começar a analisar estes serviços. Algumas questões que você pode se perguntar em relação a cada um são:

- Este serviço deve ser executado?
- Este serviço está executando em uma interface da qual ele não precisa? Ele deve estar vinculado a um único IP?
- Suas regras de firewall estão estruturadas para permitir tráfego legítimo passar para este serviço?
- Suas regras de firewall estão bloqueando tráfego que não seja legítimo?
- Você tem um método de recepção de alertas de segurança sobre vulnerabilidades para cada um destes serviços?

Esse tipo de auditoria de serviço deve ser uma prática padrão ao se configurar qualquer servidor em sua infraestrutura.

Quão difícil é implementar isto?

A realização de uma auditoria básica de serviço é incrivelmente simples. Você pode encontrar quais serviços estão escutando em portas em cada interface utilizando o comando `netstat`. Um exemplo simples que mostra o nome do programa, PID, e os endereços que estão sendo utilizados para a escuta de tráfego TCP e UDP é:

```
$ sudo netstat -plunt
```

Copy

Você verá uma saída que se parecerá com isto:

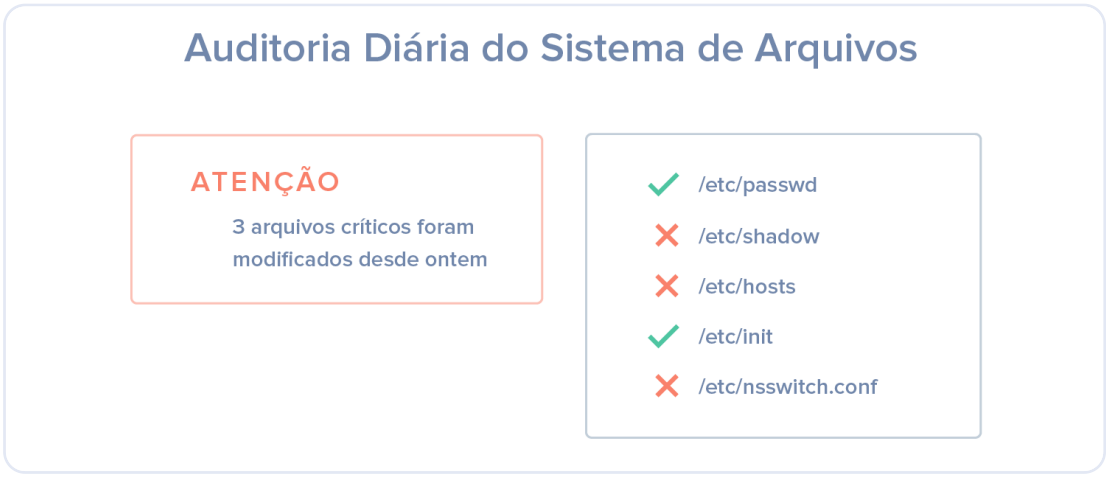
```
$ Active Internet connections (only servers)
$ Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program
$ tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      887/sshd

$ tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      919/nginx
$ tcp6       0      0 :::22                   :::*                    LISTEN      887/sshd
$ tcp6       0      0 :::80                   :::*                    LISTEN      919/nginx
```

Copy

As colunas principais que você precisa prestar atenção são `Proto`, `Local Address`, e `PID/Program name`. Se o endereço é `0.0.0.0`, então o serviço está aceitando conexões em todas as interfaces.

Auditoria de Arquivo e Sistemas de Detecção de Intrusão

A auditoria de arquivo é o processo de comparação do sistema atual contra um registro dos arquivos e as características do arquivo do seu sistema, quando ele está em um estado bom e conhecido. Isto é utilizado para detectar alterações no sistema que podem ter sido autorizadas.



Um sistema de detecção de intrusão, ou IDS, é uma peça de software que monitora um sistema ou uma rede por atividades não autorizadas. Muitas implementações IDS baseadas em host utilizam auditoria de arquivo como um método de verificar se o sistema foi alterado.

Como Ele Melhora a Segurança?

Similar à auditoria em nível de serviço acima, se você é sério sobre garantir um sistema seguro, é muito útil poder realizar auditorias em nível de arquivo do seu sistema. Isto pode ser feito periodicamente pelo administrador ou como parte de um processo automatizado em um IDS.

Estas estratégias são algumas das únicas maneiras de ter certeza absoluta de que seu sistema de arquivos não foi alterado por algum usuário ou processo. por muitas razões, invasores desejam se manter ocultos de forma que possam continuar a explorar o servidor por um longo período de tempo. Eles podem substituir binários com versões comprometidas. Fazer uma auditoria do sistema de arquivos irá lhe dizer se quaisquer dos arquivos foram alterados, permitindo que você fique confiante na integridade do seu ambiente de servidor.

Quão difícil é implementar isto?

A implementação de um IDS ou a condução de uma auditoria de arquivos pode ser um processo bastante intensivo. A configuração inicial envolve informar ao sistema de auditoria sobre quaisquer alterações não padronizadas que você fez no servidor e definir caminhos que devem ser excluídos para criar uma linha de base para leitura.

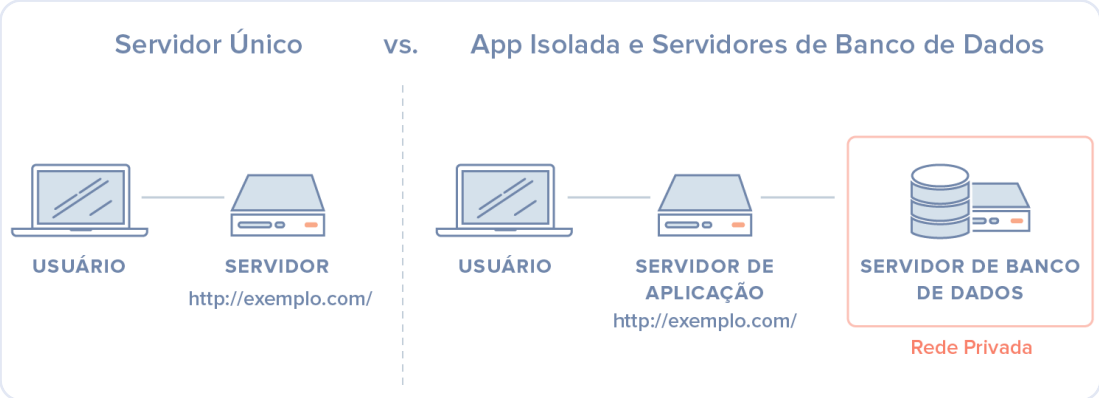
Isso também envolve mais operações do dia a dia. Isso complica os procedimentos de atualização, pois você precisará verificar novamente o sistema antes de executar atualizações e, em seguida, recriar a linha de base depois de executar a atualização para capturar as mudanças nas versões do software. Você também precisará descarregar os relatórios para outro local para que um intruso não possa alte

auditoria para encobrir suas pistas.

Enquanto isto pode aumentar sua carga de administração, ser capaz de verificar seu sistema contra uma cópia conhecida e boa é uma das únicas maneiras de assegurar que os arquivos não foram alterados sem o seu conhecimento. Alguns sistemas populares de auditoria/detecção de intrusão são o Tripwire e o Aide.

Ambientes de Execução Isolada

Ambientes de execução isolada referem-se a qualquer método no qual componentes individuais são executados dentro de seu próprio espaço dedicado.



Isso pode significar separar seus componentes de aplicativos discretos em seus próprios servidores ou pode se referir à configuração de seus serviços para operar em ambientes `chroot` ou em contêineres. O nível de isolamento depende fortemente dos requisitos da sua aplicação e da realidade da sua infraestrutura.

Como Eles Melhoram a Segurança?

Isolar seus processos em ambientes de execução individuais aumenta sua capacidade de isolar quaisquer problemas de segurança que possam surgir. Assim como os anteparos e os compartimentos podem ajudar a conter violações no casco dos navios, separar seus componentes individuais pode limitar o acesso que um invasor tem a outras partes de sua infraestrutura.

Quão difícil é implementar isto?

Dependendo do tipo de contenção que você escolher, isolar suas aplicações pode ser relativamente simples. Empacotando seus componentes individuais em contêineres, você pode alcançar rapidamente alguma medida de isolamento, mas observe que o Docker não considera sua conteinerização uma funcionalidade de segurança.

Configurar um ambiente `chroot` para cada peça também pode fornecer algum nível de isolamento, mas este também não é um método de isolamento infalível, pois muitas vezes existem maneiras de sair de um ambiente `chroot`. Mover componentes para máquinas dedicadas é o melhor nível de isolamento, e em muitos casos pode ser o mais fácil, mas pode custar mais pelas máquinas adicionais.

Conclusão

As estratégias descritas acima são apenas alguns dos aprimoramentos que você pode fazer para melhorar a segurança de seus sistemas. É importante reconhecer que, embora seja melhor tarde do que nunca, as medidas de segurança diminuem em sua eficácia quanto mais você demorar para implementá-las. A segurança não pode ser uma reflexão tardia e deve ser implementada desde o início juntamente com os serviços e aplicativos que você está fornecendo.