Saiba mais sobre os serviços do Azure que podem ser usados para ajudar a garantir a segurança, a proteção e a confiabilidade da rede.

**Objetivos de aprendizagem**

Depois de concluir este módulo, você poderá:

* Identificar as camadas que compõem uma estratégia de *defesa em profundidade*.
* Explicar como o Firewall do Azure possibilita o controle do tráfego permitido na rede.
* Configurar grupos de segurança de rede para filtrar o tráfego de rede proveniente dos recursos do Azure e destinado a eles em uma Rede Virtual do Microsoft Azure.
* Explicar como a Proteção contra DDoS do Azure ajuda a proteger os recursos do Azure contra ataques de DDoS.

**Pré-requisitos**

* Você precisa estar familiarizado com a terminologia e os conceitos básicos da computação.
* Ter noções básicas de computação em nuvem é útil, mas não é necessário.

# Introdução

Cada aplicativo e serviço, seja local ou na nuvem, precisa ser projetado tendo a segurança em mente. Há coisas demais em risco. Por exemplo, um ataque de negação de serviço pode impedir que os clientes acessem seu site ou seus serviços e impedir que você faça negócios. Seu site também poderia ser desfigurado, causando danos à sua reputação. Uma violação de dados seria ainda pior, pois poderia arruinar uma confiança arduamente conquistada, além de causar danos pessoais e financeiros consideráveis.

## Conheça a Tailwind Traders

A [Tailwind Traders](https://www.tailwindtraders.com/" \t "az-portal) é um varejista fictício de materiais para reforma e construção. A empresa opera lojas de varejo de ferragens em todo o mundo e online.

Os diferenciais da Tailwind Traders são os preços competitivos, as entregas rápidas e a ampla gama de itens. Eles estão examinando as tecnologias de nuvem para aprimorar as operações de negócios e dar suporte à expansão para novos mercados. Ao migrar para a nuvem, a empresa pretende aprimorar a experiência de compra para se diferenciar ainda mais dos concorrentes.

**Como a Tailwind Traders vai proteger suas redes?**

Conforme migra para a nuvem, a Tailwind Traders precisa avaliar suas necessidades de segurança antes de implantar uma linha de código sequer em produção.

Embora a segurança deva ser considerada em cada camada dos aplicativos da empresa (desde os servidores físicos até os dados dos aplicativos), há fatores relacionados especificamente à configuração de rede e ao tráfego de rede das cargas de trabalho baseadas em nuvem.

Neste módulo, você vai se concentrar nas funcionalidades de segurança de rede do Azure e examinar como elas ajudam a proteger suas soluções na nuvem com base em suas necessidades de negócios.

**Objetivos de aprendizagem**

Depois de concluir este módulo, você poderá:

* Identificar as camadas que compõem uma estratégia de *defesa em profundidade*.
* Explicar como o Firewall do Azure possibilita o controle do tráfego permitido na rede.
* Configurar grupos de segurança de rede para filtrar o tráfego de rede proveniente dos recursos do Azure e destinado a eles em uma Rede Virtual do Microsoft Azure.
* Explicar como a Proteção contra DDoS do Azure ajuda a proteger os recursos do Azure contra ataques de DDoS.

**Pré-requisitos**

* Você precisa estar familiarizado com a terminologia e os conceitos básicos da computação.
* Ter familiaridade com a computação em nuvem é útil, mas não é necessário.

# **O que é defesa profunda?**

Atualmente, a Tailwind Traders executa cargas de trabalho localmente, em seu datacenter. A execução local significa que a empresa é responsável por todos os aspectos da segurança, do acesso físico a edifícios até o modo como os dados são transferidos e desconectados da rede. Eles querem saber como sua estratégia atual de defesa em profundidade se compara com executar na nuvem.

O objetivo da *defesa profunda* é proteger as informações e impedir que elas sejam roubadas por pessoas que não estão autorizadas a acessá-las.

Uma estratégia de defesa em profundidade usa uma série de mecanismos para reduzir o avanço de um ataque que busca obter acesso não autorizado aos dados.

## Camadas da defesa em profundidade

Você pode visualizar a defesa em profundidade como um conjunto de camadas, com os dados a serem protegidos no centro.

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

Cada camada fornece proteção, de modo que se uma camada for violada, uma camada seguinte já estará em vigor para impedir a exposição adicional. Essa abordagem elimina a dependência de qualquer camada única de proteção. Ela desacelera um ataque e fornece telemetria de alerta sobre a qual as equipes de segurança podem agir, seja automática ou manualmente.

Aqui está uma breve visão geral da função de cada camada:

* A camada de *segurança física* é a primeira linha de defesa para proteger o hardware de computação no datacenter.
* A camada de *identidade e acesso* controla o acesso à infraestrutura e ao controle de alterações.
* A camada de *perímetro* usa a proteção contra DDoS (ataque de negação de serviço distribuído) para filtrar ataques em grande escala antes que eles possam causar uma negação de serviço para os usuários.
* A camada de *rede* limita a comunicação entre recursos por meio de controles de acesso e segmentação.
* A camada de *computação* protege o acesso a máquinas virtuais.
* A camada de *aplicativo* ajuda a garantir que os aplicativos estejam seguros e livres de vulnerabilidades de segurança.
* A camada de *dados* controla o acesso aos dados corporativos e do cliente que você precisa proteger.

Essas camadas fornecem diretrizes para ajudar você a tomar decisões de configuração de segurança em todas as camadas de seus aplicativos.

O Azure fornece ferramentas e recursos de segurança em todos os níveis do conceito de defesa em profundidade. Vamos examinar cada camada em mais detalhes:

**Segurança física**

Proteger fisicamente o acesso a edifícios e controlar o acesso ao hardware de computação no datacenter é a primeira linha de defesa.

Com a segurança física, a intenção é fornecer garantias físicas contra o acesso aos ativos. Essas garantias asseguram que outras camadas não possam ser ignoradas e que a perda ou o roubo seja tratado de maneira adequada. A Microsoft usa vários mecanismos de segurança físicos em seus datacenters de nuvem.



**Identidade e acesso**

Nessa camada, é importante:

* Controle o acesso à infraestrutura e o controle de alterações.
* Usar o SSO (logon único) e a autenticação multifator.
* Faça a auditoria de eventos e alterações.

A camada de identidade e acesso refere-se a garantir que as identidades estejam seguras, o acesso seja concedido apenas ao que é necessário e os eventos de entrada e as alterações sejam registrados.

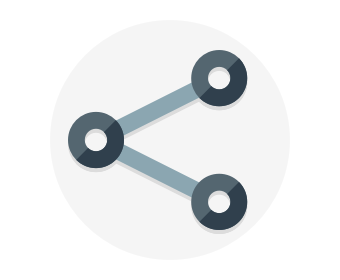


**Perímetro**

Nessa camada, é importante:

* Usar a Proteção contra DDoS para filtrar ataques em grande escala antes que eles possam afetar a disponibilidade de um sistema para os usuários.
* Use firewalls de perímetro para identificar e alertar sobre ataques maliciosos contra a rede.

O perímetro da rede trata da proteção dos recursos contra ataques baseados na rede. Identificar esses ataques, eliminar o impacto e alertar quando eles ocorrem são maneiras importantes de manter a rede segura.



**Rede**

Nessa camada, é importante:

* Limite a comunicação entre os recursos.
* Negue por padrão.
* Restringir o acesso à Internet de entrada e limitar o acesso de saída quando apropriado.
* Implemente a conectividade segura com as redes locais.

Essa camada concentra-se em limitar a conectividade de rede entre todos os recursos para permitir apenas o necessário. Ao limitar essa comunicação, você reduz o risco de uma disseminação de ataques para outros sistemas na rede.



**Computação**

Nessa camada, é importante:

* Proteger o acesso às máquinas virtuais.
* Implementar o Endpoint Protection em dispositivos e manter os sistemas atualizados e com patches.

Malware, sistemas sem patches e sistemas sem proteção adequada abrem o ambiente para ataques. Essa camada tem como foco garantir que os recursos de computação estejam seguros e que haja controles adequados em vigor para minimizar os problemas de segurança.



**Aplicativo**

Nessa camada, é importante:

* Verificar se os aplicativos estão seguros e livres de vulnerabilidades.
* Armazene os segredos de aplicativos confidenciais em uma mídia de armazenamento seguro.
* Faça com que a segurança seja um requisito de design em todo o desenvolvimento do aplicativo.

A integração da segurança no ciclo de vida de desenvolvimento do aplicativo ajuda a reduzir o número de vulnerabilidades introduzidas no código. Toda equipe de desenvolvimento deve garantir que seus aplicativos sejam seguros por padrão.



**Dados**

Em quase todos os casos, os invasores estão em busca de dados:

* Armazenados em um banco de dados.
* Armazenados em disco em máquinas virtuais.
* Armazenados em aplicativos SaaS (software como serviço), como o Office 365.
* Gerenciados por meio do armazenamento em nuvem.

Quem armazena dados e controla o acesso a eles é responsável por garantir que estejam protegidos adequadamente. É comum que requisitos regulatórios determinem os controles e os processos que precisam estar em vigor para garantir a confidencialidade, a integridade e a disponibilidade dos dados.

**Postura de segurança**

Sua *postura de segurança* é a capacidade da sua organização de se proteger e responder a ameaças de segurança. Os princípios comuns usados para definir uma postura de segurança são *confidencialidade*, *integridade* e *disponibilidade*, conhecidas coletivamente como CIA.

* **Confidencialidade**

O *princípio de privilégios mínimos* significa restringir o acesso a informações somente a indivíduos com acesso explícito, apenas no nível de que precisam para realizar seu trabalho. Essas informações incluem proteção de senhas de usuário, conteúdo de email e níveis de acesso para aplicativos e infraestrutura subjacente.

* **Integridade**

Impedir alterações não autorizadas a informações:

* + Em repouso: quando estão armazenadas.
  + Em trânsito: quando estão sendo transferidas de um local para outro, incluindo de um computador local para a nuvem.

Uma abordagem comum adotada na transmissão de dados é o remetente criar uma impressão digital exclusiva dos dados usando um algoritmo de hash unidirecional. O hash é enviado para o receptor juntamente com os dados. O destinatário recalcula o hash dos dados e o compara com o original, a fim de garantir que os dados não tenham sido perdidos nem modificados em trânsito.

* **Disponibilidade**

Garantir que os serviços estejam funcionando e possam ser acessados somente por usuários autorizados. Os *ataques de negação de serviço* são projetados para degradar a disponibilidade de um sistema, afetando seus usuários.

# Proteger redes virtuais usando o Firewall do Azure

Um firewall é um dispositivo de segurança de rede que monitora o tráfego de rede de entrada e saída e decide se deve permitir ou bloquear o tráfego específico com base em um conjunto definido de regras de segurança. Você pode criar regras de firewall que especificam intervalos de endereços IP específicos. Somente clientes com endereços IP concedidos dentro desses intervalos têm permissão para acessar o servidor de destino. Em geral, as regras de firewall também podem incluir informações de porta e protocolo de rede específicas.

Atualmente, a Tailwind Traders executa dispositivos de firewall, que combinam hardware e software, para proteger a rede local. Esses dispositivos de firewall exigem um valor de licenciamento mensal para operar, além de exigir que a equipe de TI execute manutenção rotineira. À medida que a Tailwind Traders migra para a nuvem, o gerente de TI quer saber quais serviços do Azure podem proteger tanto as redes na nuvem quanto as redes locais.

Nesta parte, você explora o Firewall do Azure.

## O que é o Firewall do Azure?

O [Firewall do Azure](https://azure.microsoft.com/services/azure-firewall) é um serviço de segurança de rede gerenciado e baseado em nuvem que ajuda a proteger recursos nas redes virtuais do Azure. Uma rede virtual é semelhante a uma rede tradicional que você operaria em seu datacenter. É um bloco de construção fundamental para sua rede privada que permite que máquinas virtuais e outros recursos de computação se comuniquem com segurança entre si, pela Internet e pelas redes locais.

Veja um diagrama que mostra uma implementação básica do Firewall do Azure:

Diagrama

Descrição gerada automaticamente

O Firewall do Azure é um firewall *com estado*. Um firewall com estado analisa o contexto completo de uma conexão de rede, não apenas um pacote individual de tráfego de rede. O Firewall do Azure apresenta alta disponibilidade e escalabilidade de nuvem irrestrita.

O Firewall do Azure fornece um local central para criar, impor e registrar políticas de conectividade de aplicativo e rede em assinaturas e redes virtuais. O Firewall do Azure usa um endereço IP público estático (inalterável) para seus recursos de rede virtual, o que permite que os firewalls externos identifiquem o tráfego proveniente de sua rede virtual. O serviço é integrado ao Azure Monitor para habilitar o registro em log e a análise.

O Firewall do Azure fornece muitos recursos, incluindo:

* Alta disponibilidade interna.
* Escalabilidade de nuvem irrestrita.
* Regras de filtragem de entrada e saída.
* Suporte a DNAT (conversão de endereços de rede de destino) de entrada.
* O registro em log do Azure Monitor.

Normalmente, você implanta o Firewall do Azure em uma rede virtual central para controlar o acesso geral à rede.

Este vídeo rápido explica como o Firewall do Azure monitora o tráfego de rede de entrada e saída com base em um conjunto definido de regras de segurança. O vídeo também explica como o Firewall do Azure se compara a dispositivos de firewall tradicionais.

**O que posso configurar com o Firewall do Azure?**

Com o Firewall do Azure, você pode configurar:

* Regras de aplicativo que definem FQDNs (nomes de domínio totalmente qualificados) que podem ser acessados em uma sub-rede.
* Regras de rede que definem endereço de origem, protocolo, porta de destino e endereço de destino.
* Regras de NAT (conversão de endereços de rede) que definem endereços IP de destino e portas para converter solicitações de entrada.

O [Gateway de Aplicativo do Azure](https://azure.microsoft.com/services/application-gateway) também fornece um firewall, chamado de *WAF (firewall do aplicativo Web)*. O WAF fornece proteção de entrada centralizada para seus aplicativos Web contra explorações e vulnerabilidades comuns. O [Azure Front Door](https://azure.microsoft.com/services/frontdoor/) e a [Rede de Distribuição de Conteúdo do Azure](https://azure.microsoft.com/services/cdn/) também fornecem serviços de WAF.

# Proteger contra ataques de DDoS usando a Proteção contra DDoS do Azure

Qualquer empresa de grande porte pode ser alvo de um ataque de rede em grande escala. A Tailwind Traders não é exceção. Os invasores podem inundar sua rede para defender uma causa ou simplesmente pelo desafio. À medida que migra para a nuvem, a Tailwind Traders quer entender como o Azure pode ajudar a evitar ataques de DDoS (negação de serviço distribuído) e outros ataques.

Nesta parte, você aprende como a Proteção contra DDoS do Azure (camada de serviço Standard) ajuda a proteger os recursos do Azure contra ataques de DDoS. Primeiro, vamos definir o que é um ataque de DDoS.

## O que são ataques de DDoS?

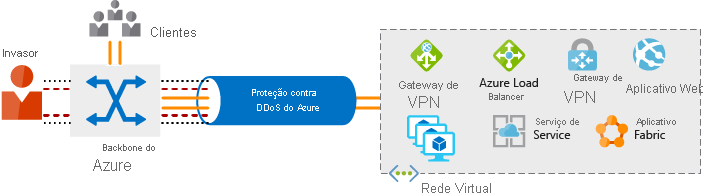
Um ataque de [negação de serviço distribuído](https://azure.microsoft.com/services/ddos-protection) tenta sobrecarregar e esgotar os recursos de um aplicativo, tornando-o lento ou sem resposta para usuários legítimos. Os ataques de DDoS podem ter como alvo qualquer recurso acessível publicamente pela Internet, incluindo sites.

## O que é a Proteção contra DDoS do Azure?

A [Proteção contra DDoS do Azure](https://azure.microsoft.com/services/ddos-protection/) (Standard) ajuda a proteger seus recursos do Azure contra ataques de DDoS.

Ao combinar a Proteção contra DDoS com práticas recomendadas de design de aplicativo, você ajuda a fornecer uma defesa contra ataques de DDoS. A Proteção contra DDoS usa a escala e a elasticidade da rede global da Microsoft para levar capacidade de mitigação de DDoS a todas as regiões do Azure. O serviço de Proteção contra DDoS ajuda a proteger seus aplicativos do Azure analisando e descartando o tráfego de DDoS na borda da rede do Azure, antes que ele possa afetar a disponibilidade do serviço.

Este diagrama mostra o tráfego de rede fluindo dos clientes e de um invasor para o Azure:



A Proteção contra DDoS identifica a tentativa do invasor de sobrecarregar a rede e bloqueia o tráfego adicional, garantindo que o tráfego nunca atinja os recursos do Azure. O tráfego legítimo dos clientes ainda flui para o Azure sem nenhuma interrupção do serviço.

A Proteção contra DDoS também pode ajudar você a gerenciar seu consumo de nuvem. Ao executar localmente, você tem um número fixo de recursos de computação. Porém, na nuvem, a computação elástica lhe permite escalar horizontalmente a implantação de modo automático para atender à demanda. Um ataque de DDoS desenvolvido de modo inteligente pode fazer com que você aumente sua alocação de recurso, gerando despesas desnecessárias. A Proteção contra DDoS Standard ajuda a garantir que a carga de rede que você processa reflita o uso do cliente. Você também pode receber crédito por qualquer custo acumulado para recursos escalados horizontalmente durante um ataque de DDoS.

## Quais camadas de serviço estão disponíveis para a Proteção contra DDoS?

A Proteção contra DDoS oferece estas camadas de serviço:

* **Basic**

A camada de serviço Básica é automaticamente habilitada de modo gratuito como parte da sua assinatura do Azure.

O monitoramento de tráfego sempre ativo e a mitigação em tempo real de ataques comuns no nível de rede fornecem os mesmos tipos de proteção usados pelos serviços online da Microsoft. A camada de serviço Básica garante que a própria infraestrutura do Azure não seja afetada durante um ataque de DDoS em grande escala.

A rede global do Azure é usada para distribuir e atenuar o tráfego de ataques entre regiões do Azure.

* **Standard**

A camada de serviço Standard fornece funcionalidades de mitigação adicionais ajustadas especificamente para os recursos de Rede Virtual do Azure. A Proteção contra DDoS Standard é relativamente fácil de habilitar e não requer alterações aos aplicativos.

A camada Standard fornece monitoramento de tráfego sempre ativo e mitigação em tempo real de ataques comuns no nível de rede. Ela oferece as mesmas defesas que os serviços online da Microsoft usam.

As políticas de proteção são ajustadas por meio do monitoramento de tráfego dedicado e de algoritmos de aprendizado de máquina. As políticas são aplicadas a endereços IP públicos associados aos recursos implantados em redes virtuais, como o Azure Load Balancer e o Gateway de Aplicativo.

A rede global do Azure é usada para distribuir e atenuar o tráfego de ataques entre regiões do Azure.

## Que tipos de ataques a Proteção contra DDoS pode ajudar a evitar?

A camada de serviço Standard pode ajudar a evitar:

* **Ataques volumétricos**

A meta desse ataque é inundar a camada de rede com uma quantidade significativa de tráfego aparentemente legítimo.

* **Ataques de protocolo**

Esses ataques renderizam um destino inacessível explorando uma vulnerabilidade na pilha de protocolos das camadas 3 e 4.

* **Ataques de camada de recurso (camada de aplicativo) (somente com o firewall do aplicativo Web)**

Esses ataques são direcionados a pacotes de aplicativo Web para interromper a transmissão de dados entre os hosts. Você precisa de um WAF (firewall do aplicativo Web) para proteger-se contra ataques L7. A Proteção contra DDoS Standard protege o WAF contra ataques volumétricos e de protocolo.

# Filtrar o tráfego de rede usando grupos de segurança de rede

Embora o Firewall do Azure e a Proteção contra DDoS do Azure possam ajudar a controlar o tráfego que pode vir de fontes externas, a Tailwind Traders também quer saber como proteger suas redes internas no Azure. Fazer isso dará à empresa uma camada extra de defesa contra ataques.

Nesta parte, você examina os NSGs (grupos de segurança de rede).

## O que são os grupos de segurança de rede do Azure?

Um [grupo de segurança de rede](https://docs.microsoft.com/pt-br/azure/virtual-network/security-overview#network-security-groups?azure-portal=true) permite filtrar o tráfego de rede proveniente dos recursos do Azure e destinado a eles em uma rede virtual do Azure. Considere os NSGs como um firewall interno. Um NSG pode conter várias regras de segurança de entrada e saída que permitem a filtragem do tráfego para e de recursos por endereço IP de origem e de destino, porta e protocolo.

## Como especificar as regras do NSG?

Um grupo de segurança de rede pode conter quantas regras forem necessárias, dentro dos limites de assinatura do Azure. Cada regra especifica estas propriedades:

| **Propriedade** | **Descrição** |
| --- | --- |
| Nome | Um nome exclusivo para o NSG. |
| Prioridade | Um número entre 100 e 4096. As regras são processadas em ordem de prioridade, sendo os números menores processados antes dos números maiores. |
| Origem ou destino | Um único endereço IP ou intervalo de endereços IP, marca de serviço ou grupo de segurança de aplicativo. |
| Protocolo | **TCP**, **UDP** ou **Qualquer**. |
| Direção | Se a regra se aplica ao tráfego de entrada ou de saída. |
| Intervalo de portas | Uma única porta ou um intervalo de portas. |
| Ação | **Permitir** ou **Negar**. |

Quando você cria um grupo de segurança de rede, o Azure cria uma série de regras padrão para fornecer um nível de linha de base de segurança. Você não pode remover as regras padrão, mas pode substituí-las criando regras com prioridades mais altas.

# Combinar os serviços do Azure para criar uma solução de segurança de rede completa

Ao considerar uma solução de segurança do Azure, considere todos os elementos da defesa em profundidade.

Aqui estão algumas recomendações sobre como combinar os serviços do Azure para criar uma solução de segurança de rede completa.

**Proteger a camada do perímetro**

A camada do perímetro refere-se a proteger os recursos da sua organização contra ataques baseados em rede. Identificar esses ataques, alertar as equipes de segurança apropriadas e eliminar seu impacto são aspectos importantes para manter sua rede segura. Para fazer isso:

* Use a Proteção contra DDoS do Azure para filtrar ataques em grande escala antes que eles possam causar uma negação de serviço para os usuários.
* Use firewalls de perímetro com o Firewall do Azure para identificar e alertar sobre ataques maliciosos contra a rede.

**Proteger a camada de rede**

Essa camada concentra-se em limitar a conectividade de rede entre todos os recursos para permitir apenas o necessário. Segmente seus recursos e use os controles de nível de rede para restringir a comunicação apenas ao que é necessário.

Ao restringir a conectividade, você reduz o risco de movimento lateral em toda a rede contra um ataque. Use grupos de segurança de rede para criar regras que definem a comunicação de entrada e saída permitida nessa camada. Aqui estão algumas práticas recomendadas:

* Limitar a comunicação entre os recursos segmentando sua rede e configurando os controles de acesso.
* Negue por padrão.
* Restringir o acesso à Internet de entrada e limite a saída quando apropriado.
* Implemente a conectividade segura com as redes locais.

**Combinar serviços**

Você pode combinar os serviços de segurança e de rede do Azure para gerenciar a segurança da rede e fornecer maior proteção em camadas. Veja algumas maneiras de combinar serviços:

* **Grupos de segurança de rede e Firewall do Azure**

O Firewall do Azure complementa a funcionalidade dos grupos de segurança de rede. Juntos, eles fornecem uma melhor segurança de rede de defesa aprofundada.

Os grupos de segurança de rede fornecem filtragem de tráfego de camada de rede distribuída para limitar o tráfego aos recursos dentro das redes virtuais em cada assinatura.

O Firewall do Azure é um firewall de rede como serviço totalmente centralizado e com estado. Ele fornece proteção no nível da rede e do aplicativo em diferentes assinaturas e redes virtuais.

* **Firewall do aplicativo Web do Gateway de Aplicativo do Azure e Firewall do Azure**

O WAF (firewall do aplicativo Web) é um recurso do Gateway de Aplicativo do Azure que fornece aos seus aplicativos Web proteção de entrada centralizada contra explorações e vulnerabilidades comuns.

O Firewall do Azure fornece:

* + Proteção de entrada para protocolos não HTTP/S (por exemplo, RDP, SSH e FTP).
  + Proteção em nível de rede de saída para todas as portas e protocolos.
  + Proteção em nível de aplicativo para HTTP/S de saída.

Combiná-los fornece mais camadas de proteção.

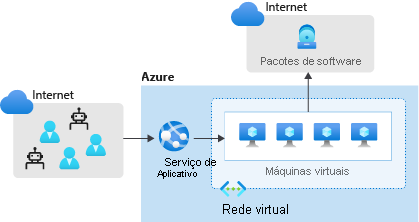
# Verificação de conhecimentos

Considere este cenário. Depois, escolha a melhor resposta para cada pergunta a seguir e selecione **Verificar suas respostas**.

A Tailwind Traders está migrando seu sistema de pagamento online para o Azure. O processamento de pedidos online começa por um site, que a Tailwind Traders gerencia usando o Serviço de Aplicativo do Azure. (O Serviço de Aplicativo é uma forma de hospedar aplicativos Web no Azure.)

O aplicativo Web que executa o site passa informações de pedido para VMs (máquinas virtuais), que continuam a processar cada pedido. Essas VMs existem em uma rede virtual do Azure, mas precisam acessar a Internet para recuperar pacotes de software e atualizações do sistema.

Veja um diagrama que mostra a arquitetura básica do sistema de pagamento da empresa:



A equipe de segurança quer garantir que apenas o tráfego de rede válido acesse os recursos do Azure da empresa. Como uma camada extra de defesa, a equipe também quer garantir que as VMs possam acessar apenas hosts confiáveis em portas específicas.

## Verificar seus conhecimentos

Parte superior do formulário

Parte inferior do formulário

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Texto, Aplicativo

Descrição gerada automaticamente

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

# Resumo

Neste módulo, você aprendeu sobre algumas das maneiras de proteger o tráfego de rede no Azure e no seu datacenter local.

*Proteção completa* é o tema recorrente. Pense na segurança como um interesse de várias camadas e de vários vetores. As ameaças vêm de locais que não esperamos e podem vir com uma força surpreendente.

Agora, a Tailwind Traders tem algumas ferramentas e serviços que pode usar para proteger suas redes. Confira abaixo um breve resumo:

* O Firewall do Azure é um serviço de segurança de rede gerenciado e baseado em nuvem que ajuda a proteger recursos nas redes virtuais do Azure.
* Uma rede virtual do Azure é semelhante a uma rede tradicional que você operaria em seu datacenter. Ela permite que máquinas virtuais e outros recursos de computação se comuniquem com segurança entre si, pela Internet e por redes locais.
* Um NSG (grupo de segurança de rede) permite que você filtre o tráfego de rede de e para recursos do Azure em uma rede virtual.
* A Proteção contra DDoS do Azure ajuda a proteger os recursos do Azure contra ataques de DDoS.