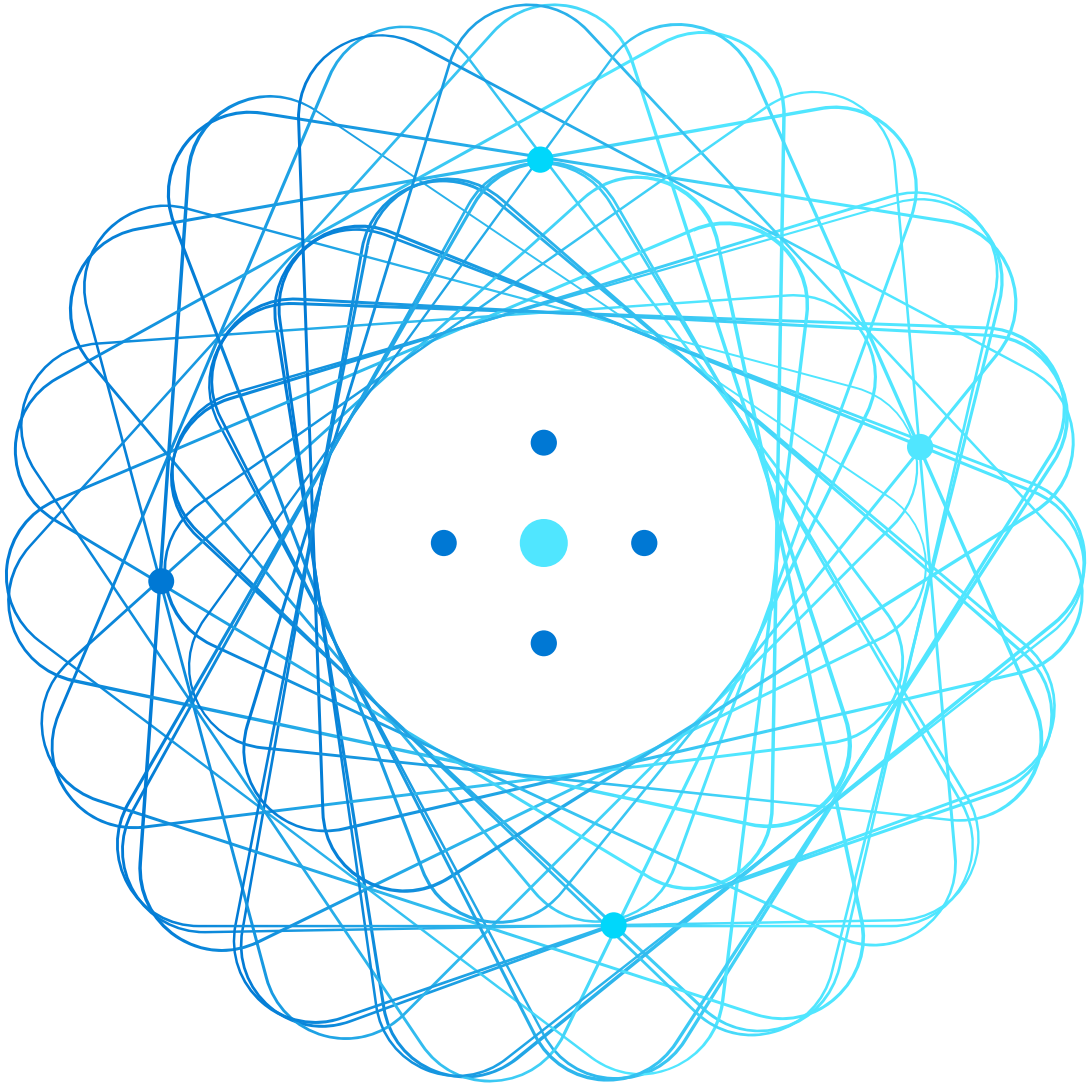
Microsoft Azure

AZ-900T0x Módulo 04: Segurança



Módulo 04 – Esboço

Você vai aprender os seguintes conceitos:

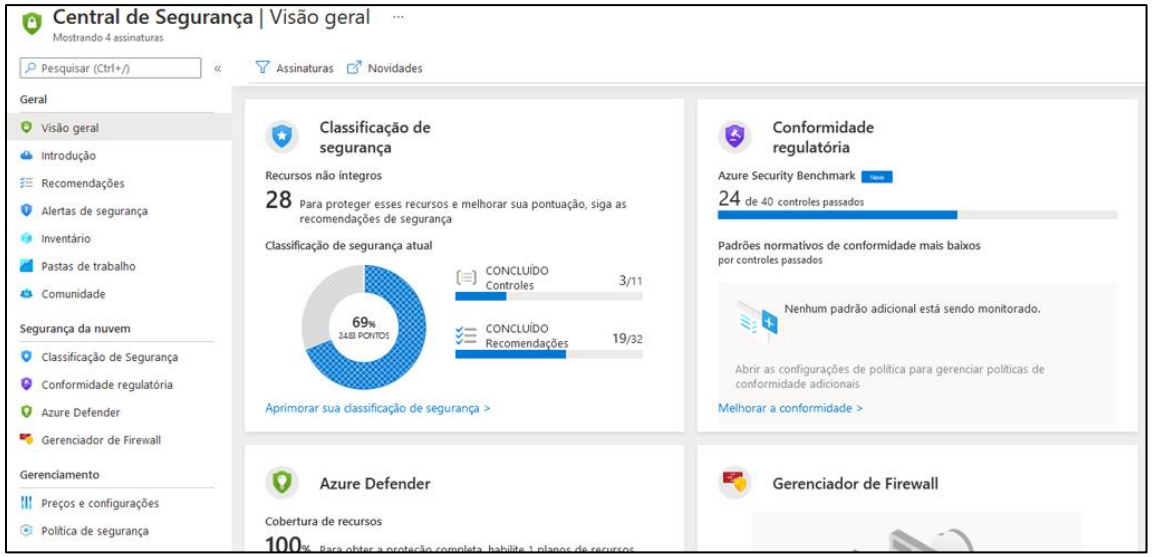
- **Recursos de Segurança do Azure**
  - Central de Segurança e limpeza de recursos
  - Key Vault, Sentinel e Hosts Dedicados
- **Segurança de rede do Azure**
  - Defesa em Profundidade
  - Grupos de Segurança de Rede e Firewalls
  - Proteção contra DDoS

Recursos e ferramentas de segurança

Central de Segurança do Azure

A Central de Segurança do Azure é um serviço de monitoramento que fornece proteção contra ameaças nos datacenters do Azure e nos datacenters locais.

- Fornece recomendações de segurança
- Detectar e bloquear malwares
- Analisar e identificar possíveis ataques
- Controle de acesso just-in-time para portas



Central de Segurança do Azure – recursos

Conformidade com a Política

Executar políticas em grupos de gerenciamento, assinaturas ou locatários.

Avaliações Contínuas

Avaliar recursos novos e implantados para garantir que eles sejam configurados corretamente.

Recomendações Personalizadas

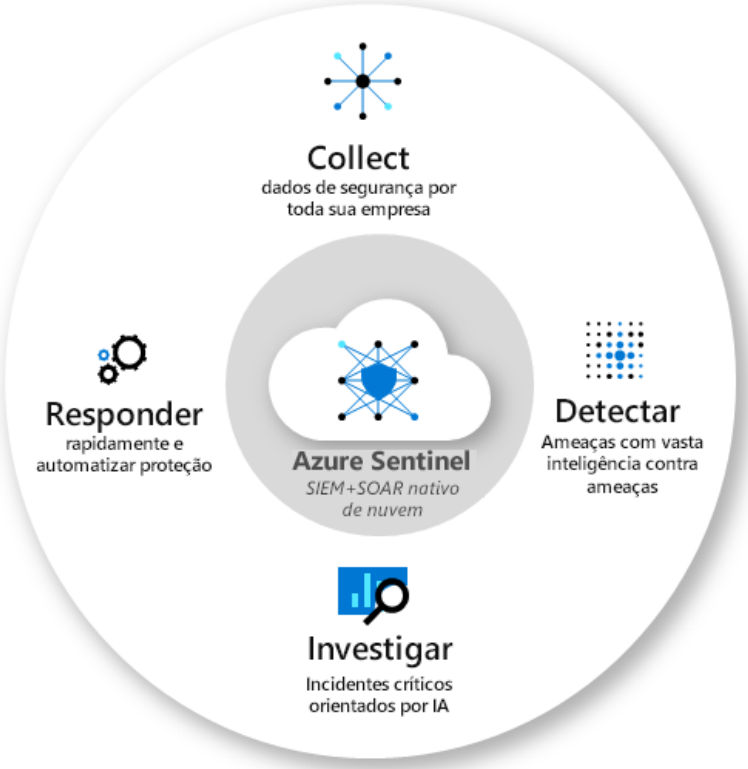
Recomendações baseadas na carga de trabalho existente com instruções sobre como implementá-las.

Proteção contra ameaças

Analisar as ameaças experimentadas por meio de alertas e relatórios de recursos afetados.

Azure Sentinel

O **Azure Sentinel** é uma solução de gerenciamento de informações de segurança (SIEM) e de resposta automatizada de segurança (SOAR) que fornece uma análise de segurança e inteligência contra ameaças em uma empresa.



Conector e Integrações:

- Office 365
- Azure Active Directory
- Proteção Avançada contra Ameaças do Azure
- Microsoft Cloud App Security

Azure Key Vault

O **Azure Key Vault** armazena segredos do aplicativo em um local de nuvem centralizado para controlar com segurança as permissões e o registro em log de acesso.

- Gerenciamento de segredos.
- Gerenciamento de chaves.
- Gerenciamento de certificados.
- Armazenar segredos apoiados por módulos de segurança de hardware (HSMs).

Conectividade de rede segura

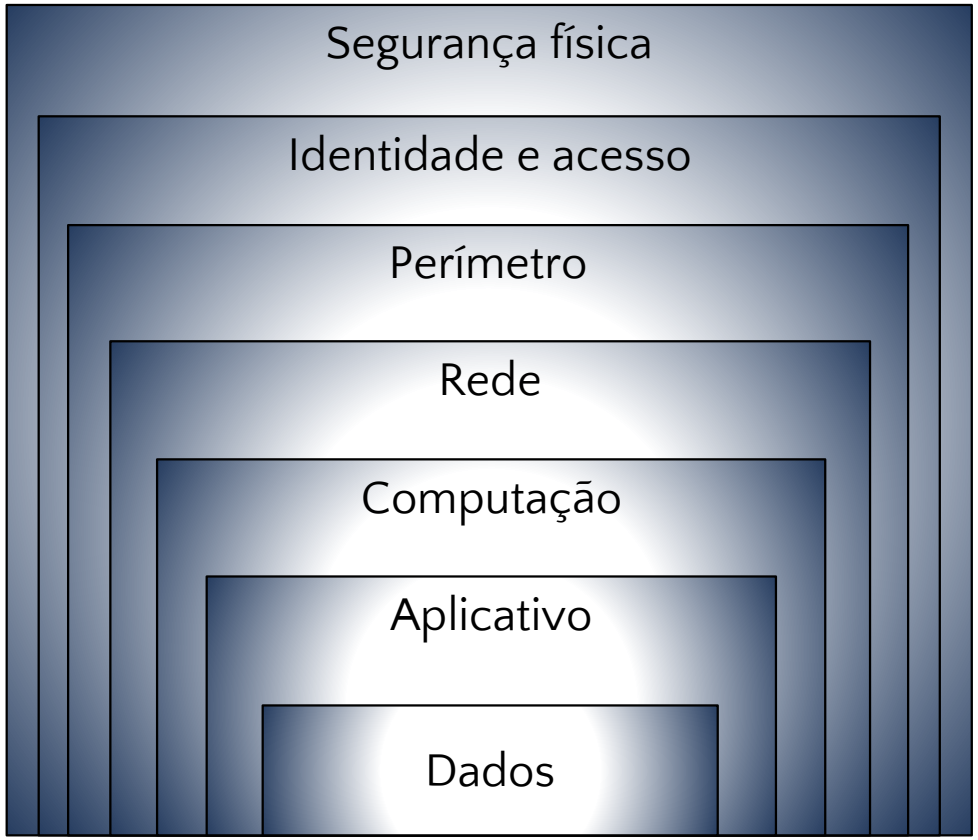
Conectividade de Rede Segura – Domínio de Objetivo

Descrever o conceito e a funcionalidade de:

- Proteção completa
- Grupos de Segurança de Rede (NSG)
- Firewall do Azure
- Proteção contra DDoS do Azure

Defesa em Profundidade

- Uma abordagem em camadas para proteger sistemas de computador.
- Fornece vários níveis de proteção.
- Ataques contra uma camada são isolados das camadas subsequentes.



Segurança Compartilhada

- Migrar de datacenters controlados pelo cliente para datacenters baseados em nuvem muda a responsabilidade pela segurança.

- A segurança se torna um interesse compartilhado entre provedores de nuvem e clientes.

Responsabilidade	No local	IaaS	PaaS	SaaS
Governança de dados e Rights Management	Cliente	Cliente	Cliente	Cliente
Pontos de extremidade do cliente	Cliente	Cliente	Cliente	Cliente
Gerenciamento de conta e acesso	Cliente	Cliente	Cliente	Cliente
Infraestrutura de identidade e diretório	Cliente	Cliente	Microsoft/ Cliente	Microsoft/ Cliente
Aplicativo	Cliente	Cliente	Microsoft/ Cliente	Microsoft
Controles de rede	Cliente	Cliente	Microsoft/ Cliente	Microsoft
Sistema operacional	Cliente	Cliente	Microsoft	Microsoft
Hosts físicos	Cliente	Microsoft	Microsoft	Microsoft
Rede física	Cliente	Microsoft	Microsoft	Microsoft
Datacenter físico	Cliente	Microsoft	Microsoft	Microsoft

Grupos de Segurança de Rede (NSGs)

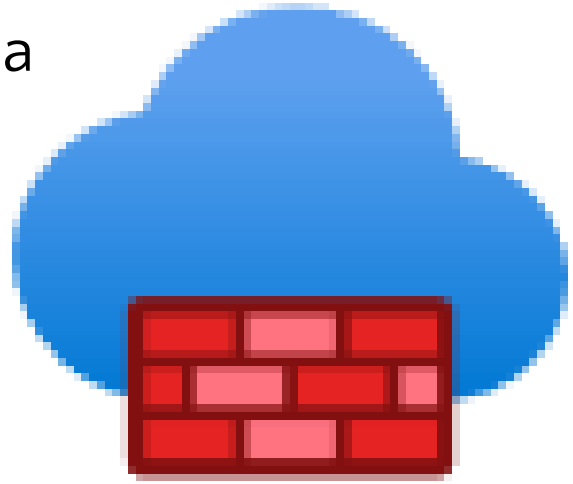
Os **Grupos de Segurança de Rede (NSGs)** filtram o tráfego de rede para os recursos do Azure (e a partir dele também) nas Redes Virtuais do Azure.

- Definir regras de entrada e de saída para filtrar por fonte e endereço IP de destino, porta e protocolo.
- Adicionar várias regras, conforme necessário, dentro dos limites da assinatura.
- O Azure aplica regras de segurança de linha de base, padrão aos novos NSGs.
- Substituir as regras padrão por regras novas e de prioridade mais alta.

Firewall do Azure

Um Firewall como Serviço com estado e gerenciado que concede/nega acesso ao servidor com base no endereço IP de origem, para proteger recursos de rede.

- Aplica regras de filtragem de tráfego de entrada e de saída
- Alta disponibilidade integrada
- Escalabilidade de nuvem irrestrita
- Usa o registro em log do Azure Monitor



O **Gateway de Aplicativo do Azure** também fornece um firewall, chamado de Firewall de Aplicativo Web (WAF). O WAF fornece proteção interna, centralizada para seus aplicativos Web.

Proteção contra DDoS (Negação de Serviço Distribuída) do Azure

Os ataques DDoS sobrecarregam e esgotam recursos de rede, tornando os aplicativos lentos ou não responsivos.

- Limpa o tráfego de rede indesejado antes que ele afete a disponibilidade do serviço.
- A camada de serviço básica é automaticamente ativada no Azure.
- A camada de serviço padrão adiciona recursos de mitigação ajustados para proteger os recursos de Rede Virtual do Azure.

Proteção Completa Analisada

Combinando soluções de segurança de rede

- **NSGs** com **Firewall do Azure** para conquistar a proteção completa.
- A **camada do perímetro** protege os limites de rede com a Proteção contra DDoS do Azure e o Firewall do Azure.
- A **camada de rede** permite que o tráfego passe entre recursos de rede apenas com as regras de entrada e de saída do Grupo de Segurança de Rede (NSG).