SESC

Relatório de Controle de Segurança e Administração do Portal

10/06/2024

SEA Tecnologia

Netskope

O Netskope é uma plataforma de segurança na nuvem que oferece uma gama abrangente de funcionalidades para proteger dados e defender contra ameaças em ambientes de nuvem e web. Aqui estão os principais aspectos de como o Netskope funciona e para que serve:

Funcionalidades do Netskope

1. **CASB (Cloud Access Security Broker)**:
    - **Visibilidade**: Fornece visibilidade sobre o uso de aplicativos SaaS e serviços na nuvem, identificando quais aplicativos estão sendo usados, por quem e como.
    - **Controle de Acesso**: Define e aplica políticas de acesso aos aplicativos na nuvem, garantindo que apenas usuários autorizados possam acessar informações sensíveis.
2. **Segurança de Dados (Data Security)**:
    - **DLP (Data Loss Prevention)**: Previne a perda de dados sensíveis ao monitorar e controlar a transferência de informações para fora da organização.
    - **Criptografia e Tokenização**: Proteger dados sensíveis em trânsito e em repouso, garantindo que apenas usuários autorizados possam acessá-los.
3. **Proteção contra Ameaças (Threat Protection)**:
    - **Inspeção de Conteúdo**: Analisa tráfego em tempo real para detectar e bloquear malware, ransomware e outras ameaças.
    - **Análise Comportamental**: Utiliza algoritmos de machine learning para detectar atividades anômalas e identificar possíveis ameaças internas e externas.
    - **Sandboxes**: Isola e testa arquivos suspeitos em um ambiente seguro antes de permitir o acesso.
4. **Segurança de Aplicativos SaaS e IaaS**:

- **API Connectors**: Integra-se diretamente com aplicativos SaaS e IaaS para fornecer visibilidade e controle sobre como os dados são usados e compartilhados.
- **Políticas Granulares**: Permite a definição de políticas detalhadas para controlar o uso e o compartilhamento de dados em aplicativos na nuvem.

5. **Segurança Web (Web Security)**:
   - **Secure Web Gateway (SWG)**: Protege contra ameaças da web, como phishing e sites maliciosos, e controla o acesso a conteúdo online.
   - **Análise de Conteúdo Web**: Bloqueia downloads de arquivos maliciosos e monitora a navegação dos usuários para garantir a conformidade com as políticas de segurança.
6. **Zero Trust Network Access (ZTNA)**:
   - **Acesso Seguro**: Implementa uma abordagem de segurança Zero Trust, onde o acesso é continuamente verificado, e apenas usuários e dispositivos confiáveis têm permissão para acessar os recursos corporativos.
   - **Acesso Adaptativo**: Ajusta dinamicamente as permissões de acesso com base no contexto do usuário, como localização, dispositivo e comportamento.

Para Que Serve o Netskope

1. **Proteção de Dados Sensíveis**:
   - Garante que dados confidenciais, como informações pessoais identificáveis (PII) e propriedade intelectual, sejam protegidos contra vazamentos e acessos não autorizados.
2. **Segurança na Nuvem**:
   - Oferece visibilidade e controle sobre o uso de aplicativos SaaS e serviços IaaS, ajudando as organizações a gerenciar e proteger seus ambientes de nuvem.
3. **Defesa Contra Ameaças**:

- Protege contra uma ampla gama de ameaças cibernéticas, incluindo malware, ransomware e ataques de phishing, mantendo os dados e os usuários seguros.

4. **Conformidade e Regulamentação**:
   - Ajuda as organizações a cumprir requisitos de conformidade, como GDPR, HIPAA e outras regulamentações de privacidade e segurança de dados, fornecendo controles e relatórios detalhados.
5. **Visibilidade e Controle**:
   - Proporciona visibilidade detalhada sobre o uso de dados e aplicativos na nuvem, permitindo que as organizações apliquem políticas de segurança eficazes e monitorem atividades suspeitas.

Como o Netskope Funciona

1. **Integração com Aplicativos e Infraestruturas de Nuvem**:
   - Utiliza conectores de API para integrar-se diretamente com aplicativos SaaS e serviços IaaS, fornecendo visibilidade e controle granulares.
2. **Cliente Netskope**:
   - Um agente leve instalado nos dispositivos dos usuários que monitora e controla o tráfego de rede em tempo real, aplicando políticas de segurança definidas.
3. **Análise de Tráfego**:
   - Inspecionar o tráfego de rede e de internet em tempo real para detectar e bloquear ameaças, e para garantir que as políticas de segurança e conformidade sejam aplicadas.
4. **Plataforma Centralizada**:
   - O portal do Netskope fornece uma interface centralizada para configurar políticas, monitorar atividades, gerar relatórios e responder a incidentes de segurança.

Em resumo, o Netskope é uma solução abrangente de segurança na nuvem que ajuda as organizações a proteger seus dados, usuários e aplicativos em um ambiente cada vez mais dependente da nuvem e da web.

Para que o Netskope possa proteger adequadamente a aplicação hospedada na Oracle Cloud, é necessário configurar o acesso à nossa Virtual Cloud Network (VCN). Isso envolve a criação de regras de firewall que liberem os IPs das redes do Netskope. Os IPs a serem liberados foram fornecidos pelo Ricardo e são os seguintes:

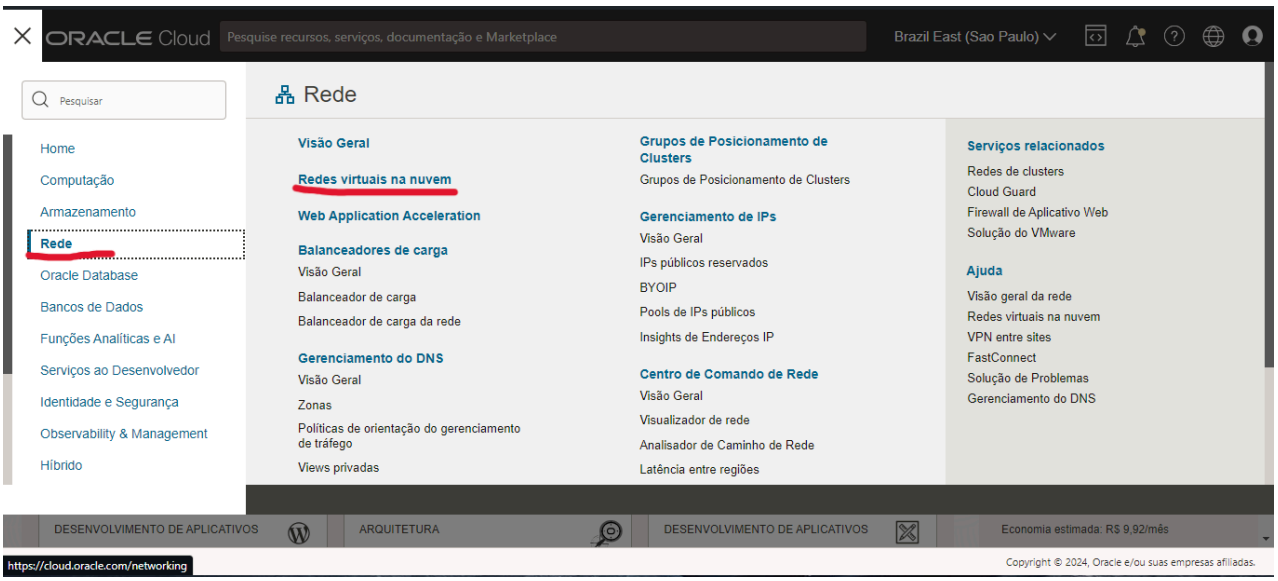
- 162.10.0.0 - 162.10.127.255
- 222.126.181.0 - 222.126.181.127
- 222.126.183.0 - 222.126.183.255
- 117.50.166.0 - 117.50.166.255
- 113.31.185.0 - 113.31.185.255
- 34.124.193.193
- 34.124.195.87
- 222.126.156.128 - 222.126.156.191
- 117.50.129.64 - 117.50.129.127
- 113.31.158.128 - 113.31.158.191
- 222.126.168.192 - 222.126.168.255
- 8.39.144.0 - 8.39.144.255
- 31.186.239.0 - 31.186.239.255
- 163.116.128.0 - 163.116.255.255
- 8.36.116.0 - 8.36.116.255

Passos para Configuração

Realizar o login ao painel da Oracle

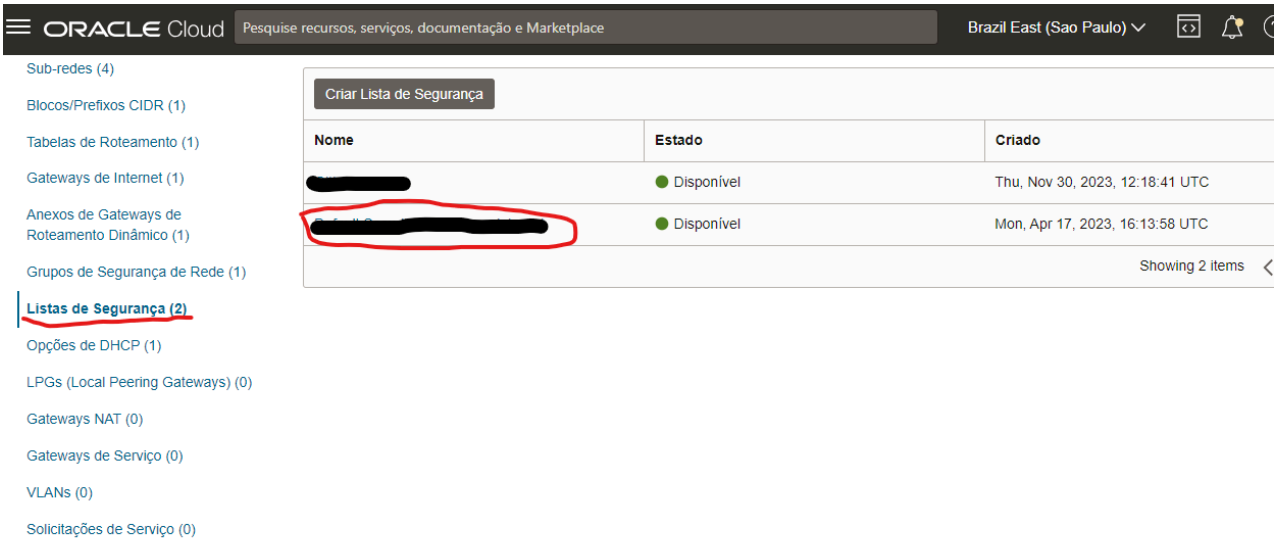
Clique no menu superior esquerdo

Clique em Rede > Redes Virtuais na Nuvem

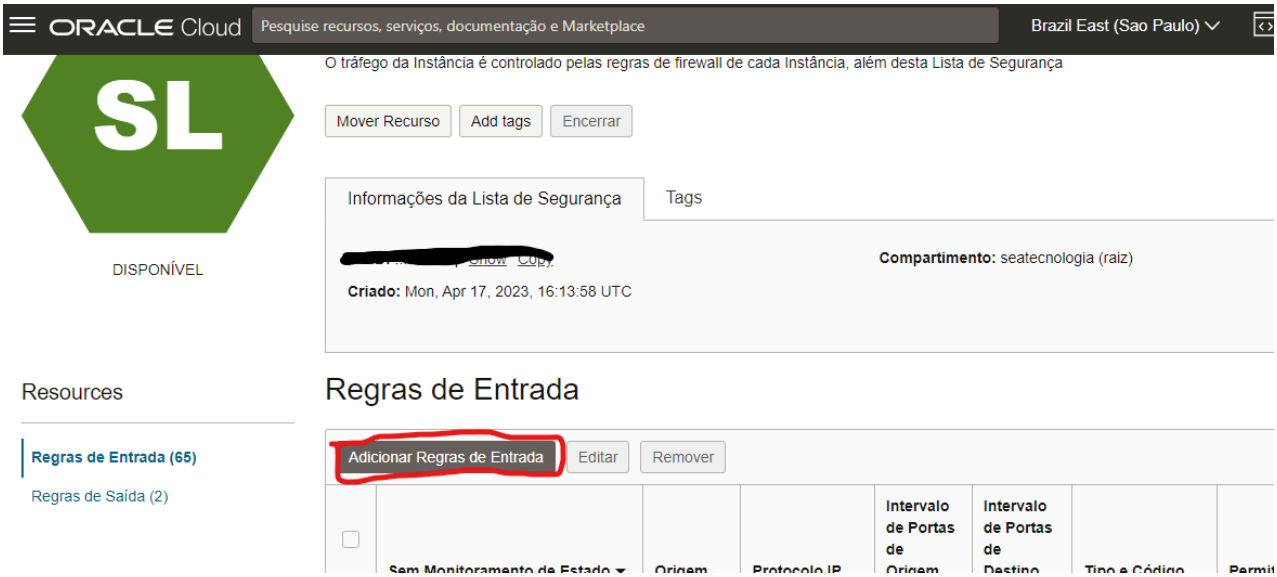


Clique na Redes Virtuais na Nuvem

Após acessar a Redes Virtuais na Nuvem role a página para baixo e clique em Lista de segurança e na lista de segurança que será utilizada para criar as regras de liberação do netskope(marcados em vermelho)



Clique em Adicionar Regras de Entrada



Regra 1: IP 162.10.0.0-162.10.127.255

Regra 2: IP 222.126.181.0-222.126.181.127

Regra 3: IP 222.126.183.0-222.126.183.255

Regra 4: IP 117.50.166.0-117.50.166.255

Regra 5: IP 113.31.185.0-113.31.185.255

Regra 6: IP 34.124.193.193

Regra 7: IP 34.124.195.87

Regra 8: IP 222.126.156.128-222.126.156.191

Regra 9: IP 117.50.129.64-117.50.129.127

Regra 10: IP 113.31.158.128-113.31.158.191

Regra 11: IP 222.126.168.192-222.126.168.255

Regra 12: IP 8.39.144.0-8.39.144.255

Regra 13: IP 31.186.239.0-31.186.239.255

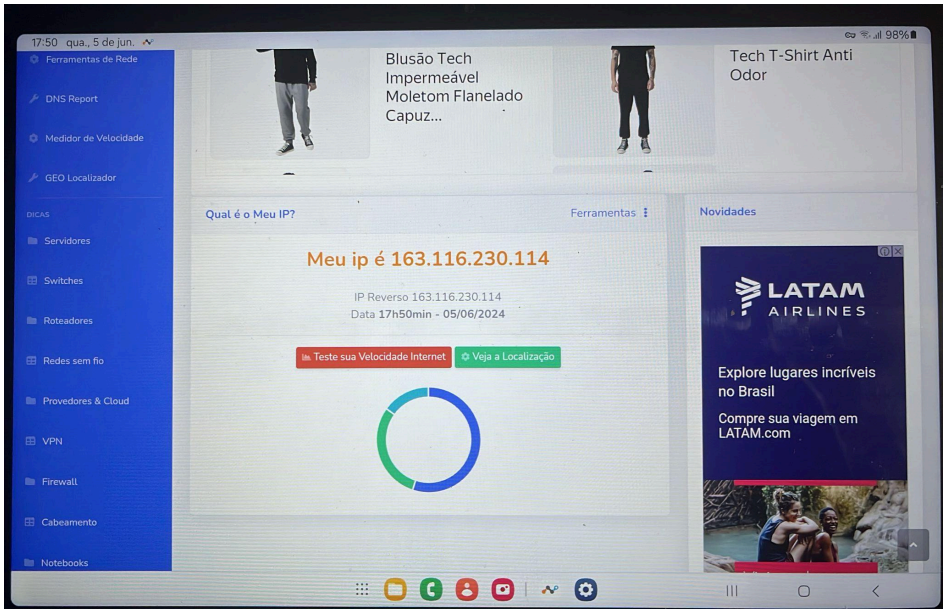
Regra 14: IP 163.116.128.0-163.116.255.255

Regra 15: IP 8.36.116.0-8.36.116.255

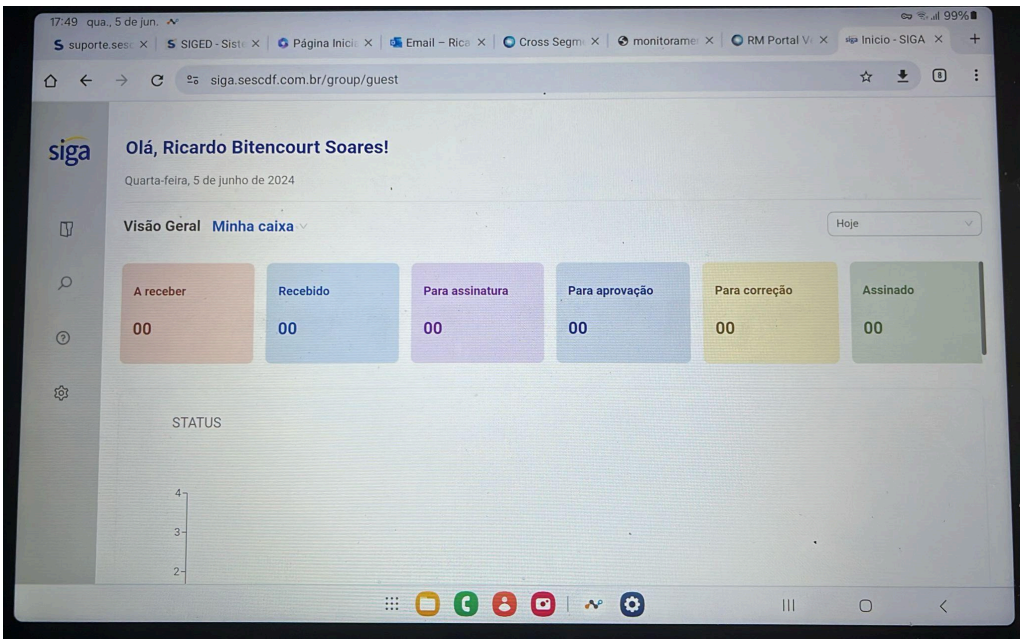
Validação do acesso

Após a configuração das regras que liberam o Netskope na rede da Oracle, foram realizados testes utilizando um tablet. Foi identificado que a configuração do Netskope e a liberação dos IPs nas regras da Oracle foram bem-sucedidas.

Abaixo temos as fotos encaminhadas mostrando a conclusão do teste, mostrando por qual IP o tablet está saindo para internet e a página da aplicação após o login mostrando que o teste foi concluído com sucesso.



Legenda: Print que identifica o dispositivo na rede da Netskope



Legenda: Print que mostra o usuário logado no sistema.