WHITEPAPER

DMZ: O QUE É, COMO FUNCIONA E COMO APLICAR ENTRE REDES TI E OT

Entenda o que é DMZ, como funciona uma DMZ industrial, jump server, historiador, acesso remoto, regras entre TI e OT, redundância, testes e erros comuns.

A3A® Engenharia de Sistemas

SUMÁRIO

Uma **DMZ** é uma zona de rede intermediária criada para hospedar serviços que precisam se comunicar com ambientes de diferentes níveis de confiança, sem permitir acesso direto entre eles. Em arquiteturas corporativas, ela costuma separar serviços expostos à internet da rede interna. Em ambientes industriais, a **DMZ OT** separa a rede corporativa dos sistemas de automação, SCADA, supervisão e controle.

O objetivo não é apenas adicionar uma VLAN chamada “DMZ”. A zona precisa possuir fronteiras controladas, regras mínimas, serviços definidos, gestão própria, monitoramento e procedimentos de acesso. Quando mal projetada, ela se torna apenas mais um segmento conectado; quando bem estruturada, reduz a possibilidade de propagação de incidentes e organiza integrações necessárias entre TI, OT, fornecedores e centros de operação.

Este artigo explica como funciona uma DMZ, quais componentes podem ser instalados nela, como controlar fluxos e quais cuidados são necessários em ambientes críticos.

1. O QUE É DMZ

DMZ é a sigla de **demilitarized zone**, ou zona desmilitarizada. Em redes, representa uma área intermediária entre zonas com diferentes níveis de confiança.

A função da DMZ é receber serviços que precisam ser acessados por mais de um ambiente, evitando que uma conexão externa alcance diretamente a rede interna ou operacional.

Exemplos:

2. COMO FUNCIONA UMA DMZ

A arquitetura aplica controles nos dois lados da zona.

Rede externa ou corporativa Fronteira de segurança DMZ Fronteira de segurança Rede interna ou OT

Cada fluxo deve possuir origem, destino, protocolo, porta, direção, finalidade e responsável. A regra recomendada é negar por padrão e liberar apenas o necessário.

A DMZ não deve permitir que um usuário utilize um serviço intermediário para alcançar livremente os sistemas protegidos. O componente hospedado nela precisa possuir função específica e controles próprios.

3. DMZ NO ROTEADOR É A MESMA COISA?

Não. Em muitos roteadores residenciais, a opção chamada **DMZ** encaminha praticamente todo o tráfego recebido da internet para um único endereço IP da rede interna. Essa função é, na prática, uma forma ampla de encaminhamento de portas e pode expor diretamente o equipamento selecionado.

Uma DMZ de arquitetura corporativa ou industrial é diferente: utiliza uma sub-rede ou zona própria, políticas de firewall, serviços intermediários, regras específicas, monitoramento e separação da rede interna. Ativar “DMZ host” em um modem ou roteador não cria essa arquitetura e não deve ser utilizado como substituto de segmentação e controle de acesso.

4. DMZ TRADICIONAL E DMZ INDUSTRIAL

A DMZ tradicional normalmente protege serviços corporativos expostos à internet. A DMZ industrial protege a fronteira entre TI e OT.

AspectoDMZ corporativaDMZ industrialFronteirainternet e rede internaTI e OTServiçosweb, e-mail, proxy, DNSjump server, historiador, logs, transferência e atualizaçãoPrioridadeconfidencialidade, integridade e disponibilidadesegurança operacional, integridade e disponibilidadeMudançasciclos mais frequentesmudanças controladas e janelas restritasImpactodados e serviços corporativosprocesso físico, supervisão e controle

Em OT, qualquer controle deve ser avaliado quanto à latência, disponibilidade e comportamento em falha.

5. DMZ NÃO É APENAS UMA VLAN

Uma VLAN cria separação lógica de camada 2, mas não define sozinha quais comunicações são permitidas, quem administra os ativos ou como eventos serão monitorados.

Uma DMZ completa precisa incluir:

Sem esses elementos, existe apenas segmentação, não necessariamente uma zona de segurança governada.

6. ARQUITETURA COM UM OU DOIS FIREWALLS

Uma DMZ pode ser implementada com um firewall de três interfaces ou com dois firewalls em série.

6.1. UM FIREWALL COM TRÊS ZONAS

A arquitetura utiliza interfaces distintas para rede externa, DMZ e rede interna.

Vantagens:

Riscos:

6.2. DOIS FIREWALLS

Um equipamento controla a entrada da DMZ e outro controla a saída para a rede protegida.

Vantagens:

Riscos:

A escolha depende do risco, criticidade, operação e padrão corporativo.

7. SERVIÇOS TÍPICOS DE UMA DMZ OT

7.1. JUMP SERVER OU BASTION HOST

É um servidor intermediário utilizado para administrar ativos da rede OT. O usuário acessa primeiro o bastion e, a partir dele, alcança somente os destinos autorizados.

O jump server pode aplicar:

7.2. RÉPLICA DE HISTORIADOR

Dados de processo podem ser replicados da OT para uma instância na DMZ. Sistemas corporativos consultam a réplica, sem acessar diretamente o historiador operacional.

A arquitetura deve definir direção do fluxo, atraso permitido, qualidade do dado e comportamento durante perda de conexão.

7.3. SERVIDOR DE TRANSFERÊNCIA DE ARQUIVOS

Arquivos de configuração, relatórios e atualizações podem ser transferidos por um repositório intermediário com análise, aprovação e rastreabilidade.

Evita-se o compartilhamento direto de pastas entre TI e OT.

7.4. PROXY DE ATUALIZAÇÃO

Servidores e estações OT podem obter atualizações a partir de um repositório controlado, sem acesso direto à internet.

O processo precisa considerar testes, homologação, janelas e retorno.

7.5. COLETORES DE LOGS

Logs podem ser consolidados na DMZ e encaminhados a SIEM ou SOC. O fluxo deve evitar que serviços corporativos iniciem conexões para ativos críticos.

7.6. SERVIÇOS DE AUTENTICAÇÃO INTERMEDIÁRIOS

Quando necessário, podem ser implantadas réplicas ou serviços específicos para reduzir dependência direta da OT em sistemas corporativos.

8. FLUXOS ENTRE TI, DMZ E OT

Uma matriz de fluxos deve ser produzida antes da configuração.

OrigemDestinoServiçoDireçãoFinalidadeUsuário autorizadojump serverHTTPS/RDP/SSH conforme políticaentradainiciar sessão de manutençãoJump serverativo OTprotocolo de administraçãocontroladasuporte autorizadoHistoriador OTréplica na DMZreplicaçãosaídadisponibilizar dados corporativosAtivos OTcoletor de logssyslog ou agentesaídaauditoria e monitoramentoProxy da DMZrepositório externoHTTPSsaídaobter pacotes aprovadosEstação OTproxy da DMZprotocolo definidosaídareceber atualização homologada

Regras genéricas entre sub-redes devem ser evitadas. O ideal é restringir por endereço, serviço, identidade e finalidade.

9. COMUNICAÇÃO INICIADA PELA OT

Sempre que possível, dados podem ser enviados da OT para a DMZ, evitando conexões iniciadas de zonas menos confiáveis para níveis críticos.

Entretanto, isso não é uma regra absoluta. Telecomandos, manutenção e autenticação podem exigir fluxos bidirecionais. O projeto deve documentar a necessidade e aplicar controles proporcionais.

Gateways unidirecionais podem ser utilizados quando a aplicação exige somente saída de dados, mas não atendem cenários que dependem de comandos ou sessões interativas.

10. ACESSO REMOTO POR MEIO DA DMZ

VPN é apenas a entrada da arquitetura. Um acesso remoto seguro deve combinar:

1. solicitação e aprovação; 2. autenticação forte; 3. conexão à VPN; 4. acesso ao jump server; 5. autorização ao ativo específico; 6. janela de tempo limitada; 7. monitoramento da sessão; 8. registro das alterações; 9. encerramento e revogação.

O fornecedor não deve possuir túnel permanente até a rede OT. Contas precisam ser individuais e vinculadas a contrato, chamado ou ordem de serviço.

11. DNS, NTP E SERVIÇOS COMPARTILHADOS

Serviços de infraestrutura podem criar dependências entre TI e OT.

11.1. DNS

A OT pode utilizar servidores próprios, réplicas ou encaminhadores controlados. A indisponibilidade do DNS corporativo não deve necessariamente paralisar funções críticas.

11.2. NTP

Fontes de tempo podem ser distribuídas por servidores intermediários. A arquitetura deve impedir que ativos críticos consultem diretamente serviços públicos sem controle.

11.3. DIRETÓRIO E IDENTIDADE

A autenticação centralizada facilita gestão, mas cria dependência. O projeto precisa considerar operação degradada, contas locais de emergência e proteção dos serviços replicados.

12. DMZ EM SUBESTAÇÕES E CENTROS DE OPERAÇÃO

Em subestações, a DMZ pode separar:

A comunicação com relés, IEDs e sistemas de proteção deve ser minimizada. Serviços de apoio não devem alcançar diretamente redes críticas sem justificativa.

13. DMZ E ARQUITETURA IEC 62443

Na IEC 62443, ativos são organizados em zonas e comunicações em conduítes. A DMZ pode funcionar como uma zona intermediária entre ambientes com requisitos de segurança diferentes.

Sua definição deve incluir:

A DMZ não substitui a análise de zonas dentro da própria OT.

14. HARDENING DOS ATIVOS DA DMZ

Por receber comunicações de diferentes ambientes, a DMZ é um alvo relevante.

Os ativos precisam de:

Um jump server comprometido pode se tornar caminho para a OT. Sua proteção deve ser proporcional ao privilégio que possui.

15. REDUNDÂNCIA E DISPONIBILIDADE

Serviços da DMZ podem ser críticos. A arquitetura deve analisar:

A redundância não deve criar caminhos paralelos não controlados. Interfaces de heartbeat, gestão e sincronização também precisam de proteção.

16. LOGS E MONITORAMENTO

Eventos importantes incluem:

Os logs precisam utilizar horário coerente e ser protegidos contra alteração.

17. PROJETO E ENTREGÁVEIS

Um projeto de DMZ pode incluir:

18. TESTES E COMISSIONAMENTO

Os testes devem comprovar:

19. ERROS COMUNS

19.1. CHAMAR UMA VLAN DE DMZ

Sem política, fronteiras, regras e gestão, existe apenas segmentação lógica.

19.2. PERMITIR ACESSO DIRETO DA TI À OT

A DMZ deve intermediar serviços e impedir conexões amplas para ativos críticos.

19.3. CONCENTRAR TODOS OS SERVIÇOS NO MESMO SERVIDOR

A consolidação pode ampliar privilégios e criar falha comum.

19.4. MANTER ACESSO PERMANENTE DE FORNECEDORES

Acesso deve ser temporário, aprovado, registrado e revogado.

19.5. NÃO CONTROLAR FLUXOS DE SAÍDA

Ativos comprometidos também podem iniciar conexões para outras zonas.

19.6. IGNORAR DEPENDÊNCIAS

DNS, NTP, identidade e certificados podem causar indisponibilidade se não houver modo degradado.

20. CONCLUSÃO

Uma DMZ organiza a comunicação entre redes de diferentes níveis de confiança. Seu valor está em impedir conexões diretas, hospedar serviços intermediários e tornar os fluxos visíveis, controláveis e testáveis.

Em ambientes TI–OT, a arquitetura precisa equilibrar segurança e disponibilidade. Jump servers, réplicas, proxies e coletores são úteis apenas quando combinados com hardening, identidade, monitoramento, redundância e procedimentos operacionais.

[1] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST SP 800-82 Rev. 3 — Guide to Operational Technology Security.

[2] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST SP 800-41 Rev. 1 — Guidelines on Firewalls and Firewall Policy.

[3] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT IEC/TS 62443-1-1:2023 — Segurança para sistemas de automação e controle industriais.

O que é uma DMZ? É uma zona intermediária entre redes com diferentes níveis de confiança, utilizada para hospedar serviços sem permitir acesso direto entre os ambientes.**Qual a diferença entre DMZ e VLAN?** VLAN é um mecanismo de segmentação lógica. DMZ inclui fronteiras, políticas, regras de acesso, ativos definidos, monitoramento e gestão.**O que é uma DMZ industrial?** É a zona que separa redes corporativas de ambientes OT, hospedando serviços intermediários como jump servers, réplicas de historiador, proxies e coletores de logs.**VPN substitui uma DMZ?** Não. VPN protege o túnel de entrada, mas não define autorização, destino, sessão, gravação, duração e intermediação até os ativos OT.**O que deve ficar em uma DMZ OT?** Serviços intermediários necessários à integração, como jump server, transferência de arquivos, réplica de historiador, proxy de atualização e coleta de logs.**É melhor usar um ou dois firewalls?** Depende do risco, da criticidade e do padrão corporativo. Dois firewalls podem aumentar separação, mas também elevam complexidade e necessidade de gestão.**Uma DMZ precisa de alta disponibilidade?** Quando seus serviços são críticos, sim. Firewalls, links, servidores e dependências devem ser analisados e testados quanto a falhas.**Como controlar fornecedores na DMZ?** Com contas individuais, MFA, jump server, aprovação, janela limitada, gravação de sessão e revogação após a atividade.**A DMZ pode hospedar NTP e DNS?** Pode hospedar ou intermediar serviços de infraestrutura, desde que dependências, redundância, segurança e operação degradada sejam planejadas.**Como testar uma DMZ?** Devem ser testados fluxos permitidos e bloqueados, autenticação, acesso remoto, failover, logs, transferência de arquivos, restauração e comportamento durante falhas.

Soluções

Serviços de engenharia

Materiais técnicos complementares

Sobre a A3A Engenharia de Sistemas

Com 30 anos de história, a A3A Engenharia de Sistemas se consolidou como referência em serviços de Engenharia, oferecendo soluções integradas de Telecomunicações, Segurança Eletrônica, Segurança Digital e Instalações Elétricas.

A empresa atua em todas as etapas do ciclo de Engenharia, desde a elaboração de projetos e consultoria técnica até a implantação, manutenção e retrofit de sistemas, sempre em conformidade com as normas técnicas e melhores práticas do setor.

A3A® Engenharia de Sistemas