WHITEPAPER

RADIUS E 802.1X: AUTENTICAÇÃO DE REDE, NAC E CONTROLE DE ACESSO EM AMBIENTES OT

Entenda RADIUS, 802.1X, supplicant, authenticator, EAP, certificados, VLAN dinâmica, NAC, equipamentos legados e aplicação em ambientes OT.

A3A® Engenharia de Sistemas

SUMÁRIO

RADIUS e IEEE 802.1X são tecnologias utilizadas para autenticar usuários e dispositivos antes de liberar acesso a redes cabeadas, Wi-Fi, VPNs e interfaces administrativas. RADIUS centraliza autenticação, autorização e accounting; 802.1X controla a porta de acesso utilizando um supplicant, um authenticator e um servidor de autenticação.

Em ambientes OT e subestações, essas tecnologias podem proteger portas de switches, redes de engenharia, Wi-Fi de manutenção e acesso administrativo. A adoção precisa considerar equipamentos legados, disponibilidade, certificados, redundância e comportamento quando o servidor de autenticação está indisponível.

Nem todo IED ou dispositivo embarcado suporta 802.1X. O projeto deve combinar autenticação forte onde possível com controles compensatórios, como portas fixas, VLANs restritas, listas de MAC, segurança física e monitoramento.

1. O QUE É RADIUS

RADIUS significa *Remote Authentication Dial-In User Service*. O protocolo centraliza decisões de autenticação, autorização e registro de uso.

Um cliente RADIUS, como switch, controlador Wi-Fi, firewall ou VPN, encaminha a tentativa de acesso ao servidor. O servidor valida a identidade e retorna aceitação, rejeição e atributos de autorização.

RADIUS não é utilizado diretamente pelo usuário final na maioria dos casos. Ele atua entre o equipamento de acesso e o serviço central de identidade.

2. O QUE É AAA

AAA representa Authentication, Authorization e Accounting.

Autenticação confirma quem é o usuário ou dispositivo. Autorização define o que pode acessar. Accounting registra início, término, endereço, porta, método e outras informações da sessão.

Separar essas funções melhora governança. Um usuário pode ser autenticado, mas receber somente acesso de leitura ou uma VLAN específica.

3. O QUE É IEEE 802.1X

IEEE 802.1X é um mecanismo de controle de acesso baseado em porta. Antes da autenticação, apenas tráfego necessário ao processo é permitido.

Após sucesso, o authenticator libera a porta conforme a política. A autorização pode incluir VLAN, ACL, perfil ou outras regras.

802.1X é aplicado em Ethernet e Wi-Fi corporativo. No Wi-Fi, está associado ao modo Enterprise e a métodos EAP.

4. SUPPLICANT, AUTHENTICATOR E AUTHENTICATION SERVER

O supplicant é o software ou dispositivo que solicita acesso. O authenticator é o switch ou ponto de acesso que controla a porta. O authentication server é normalmente um servidor RADIUS.

O authenticator não precisa conhecer a senha ou chave privada do usuário. Ele encaminha mensagens EAP entre supplicant e servidor.

A disponibilidade depende dos três elementos. Um certificado expirado no supplicant pode bloquear acesso mesmo com switch e RADIUS funcionando.

5. EAPOL E EAP

Entre supplicant e authenticator, o 802.1X utiliza EAP over LAN, ou EAPOL. Entre authenticator e RADIUS, as mensagens EAP são encapsuladas no protocolo RADIUS.

EAP é um framework que suporta diferentes métodos. A segurança depende do método escolhido e da validação de certificados.

O projeto precisa padronizar os métodos e desabilitar opções fracas ou não utilizadas.

802.1X precisa ser implantado com identidade, PKI e contingência.

Métodos EAP, certificados, perfis de porta, VLANs, ACLs e comportamento diante de falhas devem ser definidos antes da ativação obrigatória.

Conhecer a solução de Zero Trust Network Access

6. EAP-TLS

EAP-TLS utiliza certificados no cliente e no servidor. Ele oferece autenticação mútua e é uma das opções mais robustas para dispositivos gerenciados.

A implantação exige PKI, emissão, renovação, revogação e armazenamento seguro da chave privada.

Equipamentos precisam suportar o método e os algoritmos. IEDs e dispositivos OT podem ter limitações de certificado, cadeia ou tamanho de chave.

7. PEAP E MÉTODOS BASEADOS EM SENHA

PEAP cria um túnel TLS e autentica o usuário dentro dele, normalmente por credencial.

A segurança depende da validação do certificado do servidor. Se o cliente aceitar qualquer certificado, pode enviar credenciais a um servidor falso.

Métodos baseados em senha podem ser mais simples para usuários, mas exigem políticas de identidade, bloqueio e MFA em camadas complementares quando aplicável.

8. CERTIFICADOS E PKI

Certificados possuem validade, emissor, finalidade e chave privada. A operação precisa prever ciclo completo.

A PKI deve emitir certificados para RADIUS, usuários ou dispositivos conforme o método. Templates e nomes precisam ser padronizados.

A expiração simultânea de muitos certificados pode causar indisponibilidade. Monitoramento e renovação antecipada são essenciais.

O servidor NTP precisa manter horário consistente para validação e logs.

9. PORTAS RADIUS

Autenticação e autorização usam normalmente UDP 1812. Accounting utiliza normalmente UDP 1813. Portas antigas 1645 e 1646 ainda aparecem em legados.

Firewalls devem permitir apenas clientes RADIUS autorizados. Um servidor não deve aceitar solicitações de qualquer equipamento.

RADIUS tradicional utiliza segredo compartilhado entre cliente e servidor. Esses segredos precisam ser únicos, fortes e protegidos.

10. RADIUS OVER TLS

RadSec transporta RADIUS sobre TLS em arquiteturas compatíveis. Ele pode proteger melhor o transporte e facilitar relações entre domínios.

O suporte varia entre fabricantes. Não se deve presumir que qualquer switch ou controlador oferece RadSec.

Mesmo com TLS, políticas, certificados e autorização continuam necessárias.

11. AUTORIZAÇÃO DINÂMICA

O servidor RADIUS pode retornar VLAN, ACL, perfil de usuário, tempo de sessão e outros atributos.

Isso permite aplicar políticas baseadas em identidade. Um computador corporativo pode receber uma VLAN; um equipamento de manutenção, outra.

A autorização precisa ser previsível. Atributos incompatíveis ou não suportados pelo switch podem resultar em acesso inadequado ou falha.

12. VLAN DINÂMICA

VLAN dinâmica associa a porta à rede definida pelo RADIUS após autenticação.

A função reduz configuração manual, mas exige que todas as VLANs necessárias existam nos switches e enlaces.

Em OT, mudanças dinâmicas devem ser usadas com cautela. Um IED precisa permanecer na zona correta e não pode depender de uma política que varie sem controle.

13. ACL DINÂMICA

ACLs podem limitar destinos e portas conforme perfil. Isso permite acesso mais restrito que a simples associação de VLAN.

A escala depende do switch. Muitas ACLs dinâmicas podem consumir recursos de hardware.

Políticas precisam ser testadas com tráfego real e caminhos redundantes.

14. ACCOUNTING

Accounting registra início, término e atualizações da sessão. Ele apoia auditoria e investigação.

O servidor deve receber identificadores de usuário, dispositivo, switch, porta e horário. Dados incompletos reduzem utilidade.

Logs de accounting podem ser enviados a um SIEM em ambientes OT para correlação.

15. CHANGE OF AUTHORIZATION

Change of Authorization, ou CoA, permite alterar ou encerrar uma sessão após autenticação.

Uma plataforma NAC pode usar CoA quando detecta mudança de postura ou incidente.

O suporte deve ser validado. CoA mal configurado pode desconectar ativos críticos.

16. MAB E DISPOSITIVOS SEM 802.1X

MAC Authentication Bypass utiliza o endereço MAC como identidade quando não existe supplicant.

MAB é mais fraco porque MAC pode ser observado e imitado. Ele serve como mecanismo de compatibilidade, não como autenticação forte.

Em OT, pode ser combinado com porta fixa, VLAN restrita, ACL, segurança física e monitoramento de mudança.

17. ORDEM E PRIORIDADE DE AUTENTICAÇÃO

Switches podem tentar 802.1X e depois MAB, ou outra sequência. Temporizadores influenciam tempo de liberação.

Configuração inadequada pode atrasar inicialização de dispositivos ou permitir fallback desnecessário.

Cada perfil de porta deve indicar o método esperado. Portas de usuário, telefone, IED e impressora podem ter políticas diferentes.

18. MULTI-AUTH E MÚLTIPLOS DISPOSITIVOS

Uma porta pode conectar telefone e computador, switch não gerenciado ou vários dispositivos.

Modos como single-host, multi-domain e multi-auth definem quantas identidades são permitidas.

Em ambientes críticos, switches intermediários não autorizados devem ser evitados. A topologia precisa ser conhecida.

19. 802.1X EM REDES CABEADAS

No acesso cabeado, o switch bloqueia a porta até autenticação. A porta pode possuir VLAN de pré-autenticação para serviços mínimos.

Wake-on-LAN, PXE, imaging e autenticação de máquina precisam ser considerados.

Dispositivos sem usuário interativo exigem certificados de máquina ou MAB.

20. 802.1X EM WI-FI

Wi-Fi Enterprise utiliza 802.1X com controlador ou ponto de acesso como authenticator.

Certificados e validação do servidor reduzem risco de pontos falsos. SSIDs e políticas devem separar corporativo, manutenção e visitantes.

Em subestações, Wi-Fi precisa de análise de necessidade, cobertura, segurança e interferência. Nem sempre é apropriado para funções operacionais.

21. INTEGRAÇÃO COM DIRETÓRIO E IDENTIDADE

O RADIUS pode consultar Active Directory, LDAP, PKI ou provedores de identidade.

Grupos determinam autorização. Mudanças no diretório devem refletir acesso de forma controlada.

A dependência do diretório corporativo precisa ser avaliada. A rede OT não pode ficar indisponível porque um serviço remoto está inacessível sem estratégia de contingência.

22. REDUNDÂNCIA DE SERVIDORES RADIUS

Switches devem possuir servidores primário e secundário. A ordem, timeout e tentativas precisam ser configurados.

Redundância apenas no servidor não resolve perda do caminho de rede. DNS, PKI e diretório também podem ser dependências.

Testes precisam desligar cada servidor e verificar tempo de failover e comportamento das sessões existentes.

23. FAIL-OPEN E FAIL-CLOSED

Fail-closed bloqueia acesso quando autenticação não está disponível. Fail-open libera conforme política de contingência.

Nenhuma escolha é universal. Em OT, bloquear todos os ativos após perda do RADIUS pode afetar disponibilidade; liberar qualquer dispositivo pode afetar segurança.

A política pode usar VLAN crítica, autorização em cache ou lista restrita. A decisão deve ser baseada em risco e testada.

24. CRITICAL VLAN E CONTINGÊNCIA

Alguns switches oferecem VLAN crítica quando todos os servidores RADIUS estão indisponíveis.

Ela deve fornecer apenas os serviços necessários. Não pode equivaler à rede operacional completa sem controle.

O retorno ao RADIUS precisa reautenticar ou manter sessão conforme política.

25. NAC E POSTURA

NAC combina autenticação, inventário, classificação e política. Pode avaliar sistema operacional, agente, certificado ou comportamento.

Em OT, agentes nem sempre são possíveis. Classificação passiva e perfis de comunicação podem complementar.

A arquitetura de Redes Industriais deve definir onde o NAC controla e onde apenas monitora.

Equipamentos legados exigem exceções controladas, não portas abertas.

MAB, portas fixas, VLAN restrita, segurança física e monitoramento devem compensar a ausência de supplicant sem transformar a exceção em padrão.

Conhecer o serviço de Projeto de Telecomunicações

26. APLICAÇÃO EM SUBESTAÇÕES

802.1X pode proteger notebooks de engenharia, estações, servidores e portas administrativas.

IEDs com suporte podem utilizar EAP-TLS. Equipamentos legados podem usar MAB e controles compensatórios.

Portas de GOOSE, Sampled Values ou redes de processo exigem cuidado. A autenticação não deve introduzir indisponibilidade ou comportamento incompatível com o projeto IEC 61850.

27. COMPATIBILIDADE COM IEDS

O IED em subestações pode suportar 802.1X apenas em determinadas portas ou firmwares.

A documentação deve informar métodos EAP, certificados, tempo de boot e comportamento após expiração.

O teste precisa incluir reinicialização, troca de certificado, perda do RADIUS e redundância de rede.

28. PORT SECURITY E 802.1X

Port security limita MACs, mas não substitui autenticação. Pode complementar MAB e bloquear mudanças inesperadas.

Configurações rígidas podem impedir substituição emergencial de equipamento. Procedimentos precisam existir.

Eventos de violação devem ser enviados ao monitoramento.

29. SEGURANÇA DO RADIUS

Servidores RADIUS são componentes críticos. Precisam de hardening, contas administrativas protegidas, atualizações, logs e backup.

O hardening em ambientes OT orienta baseline para servidores e endpoints.

Segredos compartilhados não devem ser reutilizados. Acesso administrativo precisa de MFA e rede de gestão.

30. SEGMENTAÇÃO E FIREWALL

Clientes RADIUS ficam em redes de gestão ou acesso. Regras permitem somente UDP 1812/1813 ou transporte definido entre equipamentos e servidores.

Diretório, PKI, DNS e NTP precisam de fluxos específicos. Abrir acesso amplo para “funcionar” contraria o princípio de menor privilégio.

A DMZ entre TI e OT pode hospedar serviços intermediários quando existe dependência entre domínios.

31. LOGS E MONITORAMENTO

Logs devem registrar Access-Request, Accept, Reject, motivo, cliente, usuário e atributos.

Muitos rejects podem indicar certificado expirado, configuração incorreta ou ataque. Novos clientes RADIUS devem ser investigados.

Switches também precisam registrar mudança de estado, método, VLAN e violação.

32. PROJETO E DOCUMENTAÇÃO

O projeto deve incluir arquitetura, servidores, clientes RADIUS, métodos EAP, PKI, perfis, VLANs, ACLs, accounting e contingência.

Cada tipo de porta deve possuir template. Exceções precisam de justificativa e controles compensatórios.

A matriz de dependências inclui diretório, DNS, NTP, CA e firewall.

33. IMPLANTAÇÃO POR ETAPAS

A ativação deve começar em modo monitor ou portas piloto. Políticas são ajustadas antes de expandir.

Inventário de dispositivos evita bloqueio inesperado. Certificados precisam ser emitidos antes da exigência.

Mudanças devem possuir plano de retorno e comunicação com operação.

34. COMISSIONAMENTO E ACEITE

Os testes devem cobrir autenticação válida e inválida, autorização, accounting, redundância e contingência.

O roteiro mínimo inclui:

O Comissionamento e Aceite Técnico deve comprovar que a política não reduz indevidamente a disponibilidade operacional.

O aceite precisa testar autenticação e indisponibilidade.

Certificados, RADIUS primário e secundário, fallback, VLANs, ACLs, CoA, logs e reinicialização de dispositivos devem ser exercitados em condições reais.

Conhecer o serviço de Comissionamento e Aceite Técnico

35. DIAGNÓSTICO DE FALHAS

Timeout indica rota, firewall, segredo ou servidor indisponível. Reject exige analisar método EAP, certificado, usuário, grupo e política.

A porta presa em estado não autorizado pode indicar supplicant ausente ou EAPOL bloqueado. VLAN incorreta aponta atributo ou configuração do switch.

Falhas após renovação de certificado podem envolver cadeia, EKU, horário ou confiança.

36. ERROS COMUNS

Erros frequentes incluem ativar 802.1X sem inventário, utilizar MAB como segurança equivalente e não testar indisponibilidade do RADIUS.

Também são comuns certificados sem monitoramento, VLAN dinâmica inexistente nos enlaces e política corporativa aplicada a IEDs sem compatibilidade.

Outro erro é manter fail-open irrestrito, eliminando o controle durante falhas.

37. CONCLUSÃO

RADIUS e 802.1X permitem centralizar identidade e controlar portas de rede. EAP-TLS, VLANs, ACLs e accounting oferecem políticas mais fortes que configurações estáticas.

Em OT, a adoção precisa respeitar disponibilidade e legado. Com PKI, redundância, exceções documentadas e testes de contingência, a autenticação de rede pode reduzir conexões não autorizadas sem comprometer a operação.

[1] IEEE. IEEE 802.1X — Port-Based Network Access Control.

[2] RIGNEY, C. et al. RFC 2865 — Remote Authentication Dial In User Service (RADIUS). IETF, 2000.

[3] RIGNEY, C. RFC 2866 — RADIUS Accounting. IETF, 2000.

[4] ABBA, J. et al. RFC 5216 — The EAP-TLS Authentication Protocol. IETF, 2008.

[5] WINTER, S. et al. RFC 6614 — Transport Layer Security Encryption for RADIUS. IETF, 2012.

[6] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST SP 800-82 Rev. 3 — Guide to Operational Technology Security. Gaithersburg, 2023.

O que é RADIUS? RADIUS é um protocolo que centraliza autenticação, autorização e accounting para equipamentos de acesso à rede.**O que é 802.1X?** É um mecanismo de controle de acesso por porta que autentica usuário ou dispositivo antes de liberar a rede.**Quais são os componentes do 802.1X?** Supplicant, authenticator e authentication server, normalmente RADIUS.**O que é EAP-TLS?** É um método EAP baseado em certificados de cliente e servidor, com autenticação mútua.**Qual porta o RADIUS utiliza?** Normalmente UDP 1812 para autenticação e UDP 1813 para accounting.**O que é MAB?** MAC Authentication Bypass utiliza o endereço MAC como identidade para dispositivos sem 802.1X, com segurança inferior.**O que é VLAN dinâmica?** É a atribuição de VLAN pelo servidor RADIUS após autenticação.**O que acontece se o RADIUS falhar?** O comportamento depende da política: fail-closed, fail-open, critical VLAN ou cache. Deve ser definido e testado.**IEDs suportam 802.1X?** Alguns suportam, dependendo do modelo e firmware. Legados exigem MAB ou controles compensatórios.**Como testar 802.1X em OT?** Devem ser testados certificados, autorização, fallback, redundância, contingência, logs e reinicialização dos dispositivos.

Soluções relacionadas

Serviços relacionados

Artigos e materiais técnicos relacionados

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