WHITEPAPER

HARDENING DE SWITCHES CISCO: CHECKLIST DE SEGURANÇA, AAA, SNMP, PORTAS E GESTÃO

Checklist de hardening para switches Cisco: AAA, SSH, SNMPv3, logs, NTP, portas, VLANs, DHCP Snooping, DAI, STP, firmware e validação.

A3A® Engenharia de Sistemas

SUMÁRIO

Hardening de switches Cisco é o processo de reduzir a superfície de ataque, proteger o plano de gerenciamento, limitar serviços, controlar identidades, registrar eventos e aplicar mecanismos de segurança nas portas e protocolos de camada 2 e 3. O objetivo não é apenas “desativar comandos perigosos”, mas estabelecer uma configuração mínima segura, documentada, repetível e verificável.

Em redes corporativas e industriais, switches concentram tráfego, segmentação, autenticação e acesso a dispositivos críticos. Uma configuração inadequada pode permitir administração não autorizada, movimentação lateral, interceptação, loops, ataques de camada 2 ou perda de visibilidade. O hardening precisa ser compatível com a arquitetura e com a continuidade operacional.

Este checklist deve ser adaptado à plataforma, versão de software, licença, topologia e criticidade. Comandos e recursos variam entre Cisco IOS, IOS XE e famílias específicas. Antes de aplicar mudanças, é necessário possuir backup, acesso de contingência, janela de manutenção e plano de rollback.

1. O QUE É HARDENING DE SWITCHES CISCO

Hardening é a aplicação sistemática de controles para remover funções desnecessárias, restringir acesso e aumentar capacidade de detecção e recuperação. Em switches Cisco, ele abrange gerenciamento, identidade, serviços, protocolos, portas, logs, sincronismo, atualização e documentação.

O guia geral de hardening apresenta princípios para servidores, endpoints e OT. O switch possui particularidades: participa do encaminhamento de tráfego e pode aplicar políticas sobre os dispositivos conectados.

Uma baseline não deve ser copiada cegamente. Desativar um protocolo sem entender sua função pode interromper redundância, gerenciamento ou automação. A engenharia precisa diferenciar serviços não utilizados de serviços críticos.

2. PREPARAÇÃO ANTES DA MUDANÇA

O processo começa com inventário de modelo, número de série, versão de software, licença, localização, função, uplinks e dependências. É necessário saber quais sistemas dependem do switch e como recuperar acesso.

A configuração atual deve ser exportada e armazenada de forma protegida. Também devem ser coletados estado das interfaces, VLANs, spanning tree, rotas, vizinhanças e logs.

Mudanças em equipamentos remotos exigem caminho alternativo ou console fora de banda. Uma ACL ou alteração de AAA pode bloquear a própria equipe.

3. GESTÃO DE CONTAS E PRIVILÉGIOS

Contas compartilhadas reduzem rastreabilidade. O acesso administrativo deve utilizar identidades nominativas por AAA, preferencialmente integradas a TACACS+ ou RADIUS.

Níveis de privilégio e autorização de comandos precisam seguir menor privilégio. Operadores podem consultar estado sem poder alterar toda a configuração.

Contas locais continuam úteis para contingência, mas devem ser limitadas, protegidas e monitoradas. A senha não deve ser igual em todos os equipamentos.

O Cisco ISE pode centralizar TACACS+, políticas e accounting. Para contas críticas, PAM e jump server adicionam controle e gravação.

4. AAA, RADIUS E TACACS+

AAA separa autenticação, autorização e accounting. A configuração precisa definir ordem de servidores, timeout, tentativas e fallback.

TACACS+ é adequado para administração de dispositivos porque permite autorização granular de comandos. RADIUS é comum para acesso de rede e pode ser usado em alguns fluxos administrativos.

O fallback local deve funcionar apenas em contingência. Uma ordem incorreta pode fazer o switch depender de um servidor inacessível ou aceitar acesso local antes de consultar o AAA.

Os servidores precisam ser redundantes e sincronizados. Testes devem incluir indisponibilidade do primário e do secundário.

5. PROTEÇÃO DO ACESSO POR CONSOLE E VTY

Console, linhas VTY e interfaces de gerenciamento devem exigir autenticação. Sessões inativas precisam expirar.

O acesso remoto deve utilizar SSH. Telnet transmite credenciais e conteúdo sem criptografia e deve ser desabilitado.

A versão e os algoritmos de SSH precisam ser compatíveis com a política. Chaves antigas e cifras fracas devem ser removidas quando a plataforma permitir.

ACLs de gerenciamento devem restringir origens autorizadas. O fato de um host estar na rede corporativa não justifica acesso a todos os switches.

6. INTERFACE DE GERENCIAMENTO E VRF

O gerenciamento pode utilizar interface dedicada, SVI ou porta fora de banda. A arquitetura deve separar tráfego administrativo do tráfego operacional.

Uma VRF de gerenciamento reduz exposição e permite rotas específicas. Contudo, serviços como NTP, SNMP, syslog, AAA e DNS precisam estar associados à origem correta.

Endereços de gerenciamento não devem ser acessíveis por segmentos desnecessários. Firewalls e ACLs devem aplicar menor privilégio.

7. HTTPS E SERVIÇOS WEB

HTTP sem criptografia deve ser desativado. HTTPS pode ser mantido quando a gestão web é necessária, com certificado válido e acesso restrito.

Se a interface web não é utilizada, o serviço deve ser desabilitado. Serviços ativos sem função aumentam superfície de ataque.

Certificados precisam de ciclo de vida. Certificados padrão, autoassinados ou expirados dificultam validação e podem induzir operadores a ignorar alertas.

8. SERVIÇOS DESNECESSÁRIOS

Protocolos e serviços legados devem ser revisados. Exemplos incluem Telnet, HTTP, CDP em interfaces externas, serviços de descoberta indevidos, Smart Install em equipamentos antigos e servidores auxiliares não utilizados.

A decisão deve considerar o papel do switch. CDP pode ser útil em redes Cisco, mas não precisa ser exposto em portas que conectam terceiros ou redes não confiáveis. LLDP pode ser necessário para PROFINET ou telefonia.

Desativar serviços exige teste. Em redes industriais, um protocolo aparentemente administrativo pode ser utilizado por diagnóstico ou gerenciamento central.

Hardening eficaz começa pelo plano de gerenciamento.

AAA, SSH, ACLs, HTTPS, serviços ativos, contas locais, NTP, syslog e backups precisam ser tratados como uma baseline única e auditável.

Conhecer a solução de Endpoint Hardening

9. SNMP SEGURO

SNMPv1 e SNMPv2c utilizam community strings e não fornecem proteção criptográfica adequada. SNMPv3 com autenticação e privacidade deve ser preferido.

Views limitam quais objetos podem ser consultados. Usuários de monitoramento não precisam de acesso de escrita.

ACLs devem restringir gerentes autorizados. Traps devem ser enviados a receptores conhecidos. Comunidades padrão e reutilizadas precisam ser removidas.

O artigo sobre SNMPv3, MIB e OID detalha a arquitetura de monitoramento.

10. SYSLOG E TRILHA DE AUDITORIA

Logs devem registrar autenticações, mudanças, interfaces, spanning tree, segurança e falhas. O buffer local é útil, mas não substitui envio remoto.

Servidores syslog precisam ser redundantes e protegidos. O nível de severidade deve equilibrar visibilidade e volume.

Accounting de comandos melhora rastreabilidade. A correlação com SIEM permite detectar logins incomuns, alterações fora de janela e desativação de controles.

11. NTP E HORÁRIO CONFIÁVEL

Logs sem horário consistente perdem valor. NTP deve utilizar fontes autorizadas, com redundância e origem de interface definida.

Autenticação NTP pode ser usada quando suportada. O acesso a servidores externos deve ser controlado.

O servidor NTP em redes e subestações explica arquitetura, hierarquia e disponibilidade.

12. BACKUP E GESTÃO DE CONFIGURAÇÃO

Configurações devem ser copiadas para repositório seguro, com controle de acesso e versionamento. Backups contêm endereços, credenciais ofuscadas, comunidades e arquitetura.

A equipe precisa distinguir running-config e startup-config. Mudanças não salvas podem desaparecer na reinicialização.

Automação de backup deve validar sucesso e integridade. O processo de restauração precisa ser testado.

13. FIRMWARE, VULNERABILIDADES E CICLO DE VIDA

A versão de software precisa estar dentro do suporte. Boletins de segurança e advisories devem ser acompanhados.

Atualização não deve ser aplicada diretamente em produção sem análise. É necessário verificar memória, boot variable, compatibilidade, licença e comportamento de protocolos.

Equipamentos end-of-life representam risco crescente. Sem correções e suporte, devem entrar em plano de substituição.

14. PORTAS NÃO UTILIZADAS

Portas sem uso devem ser administrativamente desabilitadas e colocadas em VLAN sem acesso. Descrições ajudam a identificar finalidade.

Uma porta ativa e livre pode permitir conexão não autorizada. Em ambientes de campo, acesso físico também precisa ser controlado.

Quando a operação exige portas de manutenção, elas devem possuir política específica, autenticação e monitoramento.

15. VLAN NATIVA E TRUNKS

Trunks devem permitir apenas VLANs necessárias. Negociação dinâmica deve ser desabilitada quando não utilizada.

A VLAN nativa precisa ser definida e não deve transportar usuários comuns. VLAN 1 não deve ser usada indiscriminadamente para gerenciamento e produção.

Portas de acesso precisam ser explicitamente configuradas como access. Uma configuração automática pode permitir comportamento inesperado.

16. PORT SECURITY

Port security limita endereços MAC por porta e pode reagir a violações. É útil em determinados cenários, mas precisa ser aplicado com cuidado.

Telefones, hypervisors, switches downstream e equipamentos com múltiplos MACs exigem parâmetros adequados. Uma configuração rígida pode bloquear operação legítima.

Sticky MAC facilita aprendizado, porém precisa de governança. Trocas de equipamento devem atualizar a configuração.

17. 802.1X E MAB

802.1X autentica usuários ou dispositivos. MAB atende equipamentos sem supplicant, mas possui menor garantia.

A política precisa definir ordem, timeout, VLAN de falha, critical authentication e comportamento quando o servidor está indisponível.

Em OT, a implantação deve ser gradual. O artigo de RADIUS e 802.1X apresenta os cuidados para dispositivos industriais.

18. DHCP SNOOPING

DHCP Snooping diferencia portas confiáveis e não confiáveis, bloqueando servidores DHCP indevidos e construindo uma tabela de bindings.

A configuração precisa considerar uplinks, relay, Option 82 e persistência da base. Marcar a porta errada como confiável reduz o controle.

A tabela de bindings pode sustentar Dynamic ARP Inspection e IP Source Guard.

19. DYNAMIC ARP INSPECTION

DAI valida mensagens ARP com base na tabela de DHCP Snooping ou ACLs estáticas. Ele reduz ataques de ARP spoofing.

Dispositivos com IP estático exigem tratamento específico. Em redes industriais, muitos ativos não usam DHCP, portanto a implantação precisa de inventário.

Ativar DAI sem preparar bindings pode interromper comunicação.

20. IP SOURCE GUARD

IP Source Guard limita tráfego conforme bindings de endereço IP e MAC. Ele complementa DHCP Snooping.

A aplicação em portas de dispositivos estáticos precisa ser testada. Políticas inconsistentes podem bloquear endpoints legítimos.

21. SPANNING TREE E PROTEÇÃO DE TOPOLOGIA

BPDU Guard deve proteger portas onde não se espera switch. Root Guard impede que um equipamento indevido se torne raiz.

Loop Guard e UDLD podem detectar falhas específicas. A seleção depende da topologia e do meio.

PortFast reduz tempo de ativação em portas de endpoint, mas não deve ser aplicado indiscriminadamente em links entre switches.

22. STORM CONTROL

Storm control limita broadcast, multicast e unknown unicast. Ele reduz impacto de tempestades, mas thresholds inadequados podem bloquear tráfego legítimo.

Protocolos industriais e vídeo podem produzir multicast elevado. Antes de definir limites, é necessário medir o comportamento normal.

A reação pode ser descarte, shutdown ou trap. A escolha deve considerar continuidade.

23. PROTEÇÃO DE PROTOCOLOS DE ROTEAMENTO

Quando o switch executa Layer 3, vizinhanças e rotas precisam ser protegidas. Autenticação, passive interfaces, filtros e limites reduzem exposição.

Protocolos não utilizados devem ser desabilitados. Redistribuição precisa ser explicitamente controlada.

Rotas estáticas também exigem revisão e documentação. Um default route amplo pode expor redes de gerenciamento.

24. ACLS E PLANO DE GERENCIAMENTO

ACLs devem limitar SSH, HTTPS, SNMP, NTP, syslog, AAA e APIs às origens necessárias.

A ordem das regras precisa ser revisada. Uma permissão ampla no início invalida restrições posteriores.

A equipe deve testar acesso autorizado e bloqueio de origem não autorizada. Aplicar ACL remotamente sem contingência é risco elevado.

25. PROTEÇÃO DO PLANO DE CONTROLE

Control Plane Policing limita tráfego destinado ao processador. Isso reduz impacto de ataques ou tempestades.

As classes precisam considerar protocolos realmente utilizados. Limites muito baixos podem afetar roteamento, gerenciamento ou redundância.

A telemetria deve observar descartes e CPU para ajustar a política.

26. APIS, NETCONF E RESTCONF

Interfaces programáveis devem ser habilitadas apenas quando utilizadas. Elas precisam de autenticação, TLS, ACL e logs.

Contas de automação devem ter privilégio mínimo. Tokens e credenciais não devem ser gravados em scripts sem proteção.

A automação deve validar estado, erro e rollback. Uma configuração incorreta pode ser replicada em muitos switches rapidamente.

A baseline precisa respeitar a arquitetura e a continuidade operacional.

STP, DHCP Snooping, DAI, 802.1X, storm control, protocolos industriais e acesso remoto devem ser aplicados conforme a função de cada porta e switch.

Conhecer o serviço de Projeto de Telecomunicações

27. HARDENING EM SWITCHES INDUSTRIAIS CISCO

Switches industriais possuem as mesmas necessidades de gerenciamento seguro e controles adicionais ligados à continuidade OT.

Protocolos como PROFINET, EtherNet/IP, IEC 61850, PTP e redundância não devem ser afetados por ACLs ou storm control sem análise.

O artigo sobre switch industrial Cisco relaciona hardware, protocolos e segurança.

28. BASELINE E TEMPLATES

Uma baseline define configurações obrigatórias, opcionais e proibidas por classe de switch. Ela deve possuir versão e responsável.

Templates podem ser separados por acesso corporativo, distribuição, industrial, CFTV e gerenciamento. Variáveis de site são parametrizadas.

Conformidade precisa ser verificada periodicamente. O fato de o switch ter sido endurecido na implantação não garante que permaneça conforme.

29. VALIDAÇÃO PÓS-HARDENING

Após aplicar controles, deve-se verificar conectividade, redundância, protocolos, gerenciamento e monitoramento. O teste não deve se limitar ao login SSH.

O roteiro precisa comprovar que serviços desativados realmente não respondem, que logs chegam ao destino, que AAA e fallback funcionam e que portas aplicam as políticas.

Em produção, mudanças podem ser divididas em lotes para reduzir impacto.

30. CHECKLIST DE HARDENING PARA SWITCHES CISCO

O checklist mínimo inclui:

31. COMISSIONAMENTO E ACEITE

O comissionamento deve testar acessos autorizados e bloqueados, indisponibilidade de AAA, conta de contingência, logs, NTP, SNMP e serviços desativados.

Também deve verificar portas, VLANs, spanning tree, DHCP Snooping, DAI, storm control e protocolos industriais.

O Comissionamento e Aceite Técnico transforma a baseline em critérios verificáveis.

Uma baseline só é válida quando os controles são testados.

Acesso autorizado, bloqueios, fallback de AAA, logs, SNMPv3, portas, proteções de camada 2, protocolos industriais e rollback precisam ser comprovados.

Conhecer o serviço de Comissionamento e Aceite Técnico

32. ERROS COMUNS

Copiar uma configuração pronta sem entender a topologia é um erro recorrente. Outro é aplicar todos os controles de uma vez em produção.

Também são frequentes contas compartilhadas, falta de fallback, logs sem NTP e SNMPv2c mantido por conveniência.

Em OT, o maior risco é bloquear comunicação crítica por uma regra corporativa genérica. Segurança e disponibilidade precisam ser tratadas juntas.

33. CONCLUSÃO

Hardening de switches Cisco combina identidade, serviços seguros, proteção de portas, logs, atualização e governança.

Uma baseline eficaz é específica por função, validada em laboratório e aplicada com rollback. Em redes industriais, o processo precisa preservar protocolos e continuidade. Com documentação e testes, o hardening deixa de ser uma lista de comandos e passa a ser um controle de engenharia auditável.

[1] CISCO. Guide to Harden Cisco IOS Devices. Disponível em: https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html. Acesso em: 13 jul. 2026.

[2] CISCO. Cisco IOS XE Security Configuration Guides. Disponível em: https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe/products-installation-and-configuration-guides-list.html. Acesso em: 13 jul. 2026.

[3] CENTER FOR INTERNET SECURITY. CIS Cisco IOS Benchmark.

[4] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST SP 800-53 Rev. 5 — Security and Privacy Controls for Information Systems and Organizations.

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

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

[7] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 62443 series — Security for industrial automation and control systems.

O que é hardening de switch Cisco? É o processo de reduzir superfície de ataque, proteger gerenciamento, controlar identidades, limitar serviços e aplicar segurança às portas e protocolos.**Quais serviços devem ser desativados?** Serviços não utilizados, como Telnet e HTTP sem criptografia, devem ser removidos após análise de dependências.**SNMPv2c pode ser mantido?** A preferência é SNMPv3 com autenticação e privacidade. Exceções precisam ser segmentadas e documentadas.**Qual é a diferença entre RADIUS e TACACS+?** RADIUS é comum para acesso à rede. TACACS+ permite controle mais granular da administração e autorização de comandos.**Portas não utilizadas devem ser desligadas?** Sim, salvo quando existe uma finalidade de manutenção formalmente controlada.**O que é DHCP Snooping?** É um controle que diferencia portas confiáveis, bloqueia servidores DHCP indevidos e cria bindings de IP e MAC.**DAI pode afetar dispositivos com IP fixo?** Sim. Ativos estáticos precisam de bindings ou ACLs apropriadas antes da ativação.**Hardening pode interromper uma rede industrial?** Pode, se controles forem aplicados sem analisar protocolos, topologia e contingência. Por isso são necessários testes e rollback.**Com que frequência a baseline deve ser verificada?** Periodicamente e após mudanças, atualizações ou incidentes, com comparação automatizada quando possível.**Como validar o hardening?** Testando acessos, serviços, AAA, logs, NTP, SNMP, portas, proteções de camada 2, protocolos e recuperação.

Soluções relacionadas

Serviços relacionados

Identidade e acesso

Redes, monitoramento e operação

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