FTDIND

FTDIND – TELECON O&M CISCO FTD EM REDE INDUSTRIAL/IOT

40 horas **Security** **Telecon**

INTRODUÇÃO

Esse treinamento apresenta os conceitos em segurança aplicados em redes industriais/IOT, utilizando a nova geração de produtos em segurança da Cisco em NGFW/NGIPS. Através de apresentações conceituais objetivas e na realização de atividades laboratoriais intensivas em sala de aula, o profissional se habilita para as atividades de instalação, configuração, operação e suporte da solução Cisco NGFW/NGIPS FTD (Cisco® Firepower Threat Defense) e gerenciador da solução Cisco FMC (Cisco® Firepower Management Center) em ambientes industriais e IOT.

NOVIDADE: as atividades práticas são realizadas na versão 7.X do Cisco Firepower.

BR Treinamentos oferece como diferencial:
• Laboratório local, utilizando a última versão estável do produto recomendada pelo fabricante;
• Apresentamos as últimas novidades da solução;
• As atividades em laboratórios são individuais, dessa forma provendo a melhor experiência na aprendizagem (Um Pod Por Aluno).

Material Em Português: todos os nossos materiais são desenvolvidos por técnicos especialistas da área e passam por revisão técnica.

Para turmas fechadas, o treinamento pode ser adaptado e customizado as necessidades do cliente.

OBJETIVO DO CURSO

Podemos destacar os seguintes objetivos desse treinamento:

• Introdução a redes industriais e IOT;

• Introdução aos protocolos utilizados em redes industriais;

• Apresentação das práticas recomendadas em projeto e operação de redes industriais;

• Arquitetura da solução Cisco FTD e os conceitos chaves em NGFW e NGIPS;

• Configuração Inicial e Implantação da Solução;

• Configuração inicial do Cisco FTD e do Cisco FMC;

• Configuração das regras de NAT e Política em QoS;

• Configuração e utilização da ferramenta Network Discovery (Hosts, Applications & Services);

• Configuração e utilização de objetos para as configurações das políticas;

• Utilização da proteção denominada de “Security Intelligence” da Solução;

• Implantação das Políticas para a Proteção de Malware (AMP)

• Implantação e Gerenciamento das Políticas de IPS;

• Utilização e integração do Firepower Management Center;

• Configuração e utilização das ferramentas para gerenciamento das contas de usuários administrativos;

• Configuração de Soluções em VPN Site-to-Site ;

• Configuração de Soluções em VPN Remote-Access com Cisco Anyconnect;

PÚBLICO-ALVO

Voltado para profissionais que buscam conhecimentos na operação e administração do Cisco FTD NGFW & NGIPS e Gerenciador Cisco FMC em ambientes de rede industrial.

PRÉ-REQUISITOS

Para maior aproveitamento é recomendado que o aluno possua:

• Conhecimentos básicos em redes industriais e seus protocolos;

• Conhecimentos básicos em redes IP.

CONTEÚDO PROGRAMÁTICO

Introdução a redes Industriais/IoT

• Tipos de Redes Industriais e IoT
• Rede de Produção Conectada (Cisco IoT Connected Factory)
• Convergência de redes industriais e IoT
• Necessidades da Segurança Aplicada em Redes Industriais e IoT
• Vulnerabilidades Comuns em Redes Industriais e IoT
• Redes Corporativas e Components
• Redes Industriais/IoT e Seus Componentes
• Redes Industriais de Camada 2: Switching
• Redes Industriais de Camada 3: Routing
• Redes Industriais: Wireless
• Segurança Física
• Automação Industrial e Sistemas de Controle
• Modelo “Purdue”

Revisão dos Requerimentos Em Segurança de Redes Industriais e IoT

• Segurança Física
• Segurança Aplicada em Servidores e PC’s
• Melhores Práticas em Controle de Acesso
• Autenticação Baseada em Equipamentos
• Segmentação de Rede: Zonas
• Segmentação Física
• Segmentação Lógica e VLANs
• Benefícios de Segmentação VLAN para Redes Industriais e IoT
• Utilização de Listas de Controle de Acesso (ACLs)
• Rede DMZ em Redes Industriais
• Papel do Firewall em Arquitetura Industrial DMZ
• Proteção da Camada “Edge”
• Utilização de VPNs: Remote Access
• Papel da VPN em Ambientes de Redes Industriais
• Monitoramento de Rede: SIEM
• Tecnologias de Segurança Aplicadas em Redes Industriais
• Princípios de Segurança: OT
• Princípios de Segurança: IT
• Comparação: Tecnologias de Segurança e Operação IT

Revisão dos Protocolos em Redes Convergentes Industriais e Corporativas

• Protocolos Utilizados em Redes Convergentes Industriais
• Utilização de Segmentação e seus Protocolos
• Protocolos de Redundância em Camada 2
• Protocolos IPv4 e IPv6
• Outros Protocolos TCP/IP
• Roteamento IP em Redes Convergentes Industriais e IoT
• Alta Disponibilidade e seus Protocolos em Redes Convergentes Industriais e IoT
• Protocolos “Fieldbus”
• Protocolo MODBUS e suas Versões
• Protocolo DNP: Distributed Network Protocol 3
• Segurança em DNP3
• Protocolos Ethernet de Redes Industriais

• Protocolo CIP: Common Industrial Protocol
• Protocolo PROFINET
• Protocolos do Tipo Back-end
• Especificações OPC
• Segurança em Protocolos de Gerência
• Configuração dos Protocolos de Gerência
• Protocolos: NTP, IEEE 1588 PTP, Syslog over TLS/DTLS
• Protocolos de Transporte Seguros
• IPsec Protocol
• IKE Versão 2
• Protocolo ESP: Encapsulation Security Payload
• Protocolo: SSL & TLS
• Protocolo para Autenticação Segura
• Protocolo IEEE 802.1X
• Protocolo EAP: Extensible Authentication Protocol
• Protocolo IEEE 802.1AR (Secure Device Identity)

Revisão: Ameaças e Vulnerabilidades em Ambiente Industrial

• Metodologias de Ataques
• Vulnerabilidades de Protocolos Industriais
• Vulnerabilidades de Equipamentos e Servidores
• Vulnerabilidades em Segurança Física
• Equipamentos tipo “Rogues”
• Problemas Comuns em Implantação de Redes Industriais & IoT
• Ameaças do Tipo “Malware”
• Classificação de Ataques
• Ataques do Tipo “Spoofing”
• Ataques do Tipo “Man-in-the-Middle”
• Ataques do Tipo “Smurf”
• Ataques do Tipo “Buffer Overflow”
• Ataques ao Protocolo IP
• Ataques ao Protocolo TCP
• Ataques ao Protocolo UDP
• Ataques ao Protocolos Industriais: MODBUS
• Ataques ao Protocolos Industriais: DNP3
• Ataques ao Protocolos Industriais: OPC
• Ataques ao Protocolos Industriais: CIP
• Ataques ao Protocolos Industriais: ICCP
• Ataques ao Protocolos Industriais: Outros Protocolos
• Ataques Stuxnet: Malware
• Ataques Mirai: Malware

Melhores Práticas: Processos em Segurança de Redes Industriais & IoT

• Projeto e Design: Princípios em Segurança de Redes Industriais
• Práticas Recomendadas em Redes Industriais (Security Framework)
• Práticas: Células, Zonas e Áreas
• Proteção da Infraestrutura e Funções Chaves da Rede Industrial & IoT
• Práticas: Zona Industrial
• Práticas: Zona Corporativa
• IDMZ e suas Características

• Modelo Convergente em Segurança para Indústria
• Controle de Acesso: Entre Rede Corporativa e Zona IDMZ
• Controle de Acesso: Entre IDMZ e Zona Industrial
• Política de Segurança Aplicada para a Zona IDMZ
• Proteção dos Ativos Industriais

Solução Cisco Firepower Threat Defense

• Tecnologias Empregadas em Função Firewall e IPS
• Solução Cisco de Segurança em Redes Industriais
• Cisco Firepower Threat Defense: Funções e Características
• Família de Produtos Cisco Firepower
• NGFW Industrial: Cisco ISA-3000 FTD
• Licenciamento do Cisco Firepower Threat Defense
• Cisco FXOS e Cisco Firepower Device Manager
• Cisco FMC no Gerenciamento Centralizado Firepower
• Configuração da Solução e Política de Monitoramento (Health Policy)
• Opções em Alta Disponibilidade da Solução Cisco Firepower

Implantação do Cisco FTD em Projetos de Redes Industriais & IoT

• Processamento dos Pacotes pelo Cisco Firepower Threat Defense
• Diferencial Cisco Firepower: Implantação da Função “Network Discovery”
• Utilização das Políticas em NAT (Básica e Avançada)
• Configuração das Políticas de Controle (Access Control Policies)
• Implantação da Função em QoS
• Implantação da Função em Inspeção do Tráfego
• Monitoramento e Análise do Tráfego (Connection Events)
• Diferencial Cisco Firepower: Utilização da Função “Security Intelligence”
• Inspeção de Tráfego Tunelado TLS/SSL (SSL Policies)
• Inspeção da Transferência de Arquivos pela Rede (Malware Protection & File Policy)
• Inspeção do Tráfego na Detecção de Intrusão (Intrusion Prevention)
• Proteção do Tráfego Transportado pela Rede (VPN Site-to-Site)
• Proteção do Acesso Remoto pela Rede (Remote-Access VPN)
• Administração da Solução Cisco Firepower

Atividades de laboratório

Atividade 1: Acesso LAB Telecon FTD

Recursos Requiridos

Recursos de acesso provisionados

Topologia do laboratório Cisco FTD Telecon

Atividade 2: Primeiro acesso ao Cisco FMC

Tarefa 1: Acessando o Cisco FMC

Tarefa 2: Validando a configuração inicial do Cisco FMC

Atividade 3: Configuração de uma política básica

Tarefa 1: Configurando FTD Security Zones

Tarefa 2: Configurando uma ACP (Access Control Policy) básica

Tarefa 3: Configurando uma política de NAT (Zona Inside para Zona Outside)

Tarefa 4: Configurando uma política de NAT (Zona Inside para Zona DMZ)

Atividade 4: Implantando o Cisco FTD NGFW

Tarefa 1: Validando o registro do Cisco FTD com o Cisco FMC

Tarefa 2: Configuração das interfaces e rota padrão do Cisco FTD

Tarefa 3: Aplicação da política de NAT no Cisco FTD pelo Cisco FMC

Tarefa 4: Configuração das parametrizações do Cisco FTD (Platform Settings)

Tarefa 5: Modificação da política de descobertas (Network Discovery)

Tarefa 6: Modificação da política de monitoramento de ativos (Health Policy)

Tarefa 7: Modificação da política de sistema (System Policy)

Tarefa 8: Aplicação das alterações das configurações

Tarefa 9: Performando testes de implantação do Cisco FTD em camada 3

Atividade 5: Políticas avançadas em NAT e roteamento

Tarefa 1: Configuração dos objetos das políticas

Tarefa 2: Configuração de rotas estáticas

Tarefa 3: Modificação da ACP para permissão do acesso externo (Rede Outside)

Tarefa 4: Configuração de roteamento dinâmico (OSPF)

Tarefa 5: Aplicação das alterações das configurações

Tarefa 6: Performando testes das configurações avançadas

Atividade 6: Configuração da política de QoS (limitação de fluxos)

Tarefa 1: Dimensionando a linha de base comparativa dos fluxos

Tarefa 2: Configuração das limitações dos fluxos

Tarefa 3: Performando testes das configurações de limitação dos fluxos

Tarefa 4: Remoção da política de limitação dos fluxos

Atividade 7: Implantação do serviço Cisco Firepower Security Intelligence

Tarefa 1: Configuração e atualização do recurso Security Intelligence (Cisco Feeds)

Tarefa 2: Utilização da do serviço Security Intelligence (Global Deny Lists)

Tarefa 3: Aplicação das configurações e atualizações realizadas

Tarefa 4: Testes e validação das atualizações realizadas (Security Intelligence Feeds)

Tarefa 5: Configuração do serviço URL-Based Security Intelligence

Tarefa 6: Aplicação dos serviços Cisco Intelligence Feeds

Tarefa 7: Verificação e testes com o serviço URL-Based Security Intelligence

Atividade 8: Configuração e aplicação da \"ACP Decryption Policy\"

Tarefa 1: Geração de certificado (Tipo RA) para o Cisco FTD

Tarefa 2: Instalação do certificado RA gerado no Cisco FTD

Tarefa 3: Configuração da política SSL (Decryption Policy)

Tarefa 4: Adição da política SSL POLICY junto a ACP

Tarefa 5: Aplicação e testes da política SSL

Atividade 9: Configuração do controle de arquivos e Network AMP

Tarefa 1: Configuração da política de inspeção de arquivos (File Policy)

Tarefa 2: Adição da política de inspeção de arquivos junto a ACP

Tarefa 3: Testes e validação da política de inspeção de arquivos

Atividade 10: Configuração do serviço Cisco Firepower NGIPS

Tarefa 1: Configuração da política Cisco Firepower NGIPS

Tarefa 2: Atualização e ajuste da política NGIPS baseada nas recomendações (Firepower Recommendations)

Tarefa 3: Aplicação e teste da política NGIPS atualizada no Cisco FTD

Atividade 11: Configuração de solução VPN Site to Site

Tarefa 1: Configuração de VPN Site-To-Site pelo Cisco VPN Wizard

Tarefa 2: Configuração da política de NAT para VPN Site-To-Site

Tarefa 3: Configuração de rota estática para a VPN Site-To-Site (Router Peer)

Tarefa 4: Configuração da ACP para permissão de conexões VPN Site-To-Site

Tarefa 5: Teste e validação da configuração VPN Site-To-Site

Atividade 12: Administração da Solução Cisco Firepower: Parte 1

Tarefa 1: Agendamento de tarefas (Aplicação de ACP)

Tarefa 2: Automatizando o procedimento \"Firepower Recommendations\"

Atividade 13: Administração da Solução Cisco Firepower: Parte 2

Tarefa 1: Adicionando contas locais administrativas

Tarefa 2: Testando contas locais administrativas

Tarefa 3: Configurando a permissão de acesso escalado administrativo

Tarefa 4: Configurando a integração de bases externas para autenticação/autorização

Tarefa 5: Testando contas externas administrativas

Atividade 14: Configuração de Alta Disponibilidade do Cisco FTD

Tarefa 1: Configuração do recurso \"Cisco FTD HA Failover\" utilizando \"HA Wizard\" no FMC

Tarefa 2: Verificando e editando a configuração de \"HA Failover\" (Interfaces e tempos)

Tarefa 3: Performando testes da solução Cisco FTD HA Failover

Atividade 15: Utilizando os recursos do FMC para análises

Tarefa 1: Realizando análises referente a política de inspeção de arquivos

Tarefa 2: Realizando análises dos eventos da ACP

Tarefa 3: Utilizando as ferramentas Cisco Firepower Context Explorer