FTD (CISCO FIREPOWER THREAT DEFENSE FTD NGFW & NGIPS)

Objetivo

Esse curso apresenta e introduz os conceitos em segurança aplicados na nova geração de produtos da Cisco em Firewall e IPS (NGFW e NGIPS). Através de apresentações conceituais objetivas e na realização de atividades laboratoriais intensivas o profissional vai se habilitar na instalação, configuração e operação do Cisco FTD, análises dos eventos e aprimoramento e ajuste do NGIPS. Podemos destacar os seguintes objetivos desse treinamento: • Descrição do Cisco FTD e os conceitos chaves em NGFW e NGIPS • Realizar as atividades em configuração na implantação da solução • Configuração inicial do Cisco FTD e do Cisco Firepower Management • Configurar NAT e QoS • Configuração e utilização da ferramenta Network Discovery (Hosts, Applications & Services) • Configuração e utilização de objetos para as configurações das políticas • Utilização das características de “Security Inelligence” • Implantação do controle avançado para a proteção de Malware (AMP) • Implementar e gerenciar as políticas de IPS • Utilização e integração do Firepower Management Center • Configuração e utilização das ferramentas para gerenciamento das contas de usuários administrativos • Procedimentos de suporte para o FTD

Público Alvo

Voltado para profissionais que buscam conhecimentos na operação e administração do Cisco FTD NGFW & NGIPS.

Pré-Requisitos

Para maior aproveitamento é recomendado que o aluno possua • Conhecimentos básicos em seguração; • CCNA R&S ou conhecimentos equivalentes.

Carga Horária

40 horas (5 dias).

Conteúdo Programático

Conceitos Básicos de Firewall NGFW
• Conceitos de Firewall
• Tipos de Firewall
• Evolução da solução e conceitos modernos em NGFW

Conceitos Básicos de NGIPS
• Conceitos de IPS e IDS
• Evolução da solução e conceitos modernos em NGIPS

Apresentação da família de produtos Cisco
- Portfólio de Produtos
- Diferenciais da Solução
- Integração com outras soluções (PxGrid)
- Cisco ASA Firewall, ASAv e FTD
- Licenciamento da Solução

Design e aplicações do Cisco FTD NGFW e NGIPS
- Projetos e aplicações do Cisco FTD NGFW e NGIPS
- Projetos de Migração
- Projetos Novos
- Exemplos

Recomendações e Procedimentos Para Upgrade
- Procedimentos recomendados

Instalação e configuração inicial do Cisco FTD
- Produtos e cuidados para instalação
- Check-List para configuração
- Procedimentos para instalação
- Configuração inicial
- Solução Firewall Transparent ou Routed
- Integração com o Cisco Firepower Management
- Utilização do ASDM InBox

Instalação e configuração inicial do Cisco Firepower Management
- Produtos e cuidados para instalação
- Check-List para configuração
- Procedimentos para instalação
- Configuração inicial
- Integração do Cisco FTD e Cisco Firepower Management
- Procedimentos de configurações iniciais

Configuração das interfaces e inserção em uma rede em camada 3
- Configuração das interfaces
- Utilização das Zonas de Interfaces
- Parametrizações necessárias, recomendadas e opcionais

Configuração das regras de NAT
- Conceitos de NAT empregados no Cisco FTD
- Configurações de regras de NAT
- FTD e Tabela de NAT
- Verificação das regras utilizadas

Configuração do Network Discovery
- Conceitos de “Network Discovery” no FTD
- Configuração e utilização
- Verificação das descobertas

• Customizações

Utilização e configuração das regras de controle de acesso (Access Control Policies)
• Conceitos de controle de acesso no Cisco FTD
• Estrutura e design das políticas e regras
• Conceitos das regras de acesso e sua aplicação no Cisco FTD
• Configuração e aplicação das políticas de acesso

Utilização do Security Intelligence
• Conceitos de Security Intelligence
• Aplicações no Cisco FTD
• Configuração e utilização
• Suporte

Configuração e Utilização do AMP (Malware Protection)
• Conceitos de AMP
• Aplicações do AMP no Cisco FTD
• Configurações das regras e utilização na rede
• Exemplos de aplicações

Configuração e Utilização do NGIPS
• Conceitos de NGIPS aplicados no Cisco FTD
• Configuração e utilização
• Customizações e ajustes na base de regras
• Utilização das recomendações do Firepower Management
• Suporte

Utilização Das Políticas de Análise em Rede (Network Analysis Policies)
• Conceitos aplicados no Cisco FTD
• Configuração e utilização
• Utilização da base de informações
• Suporte

Administração da Solução
• Configuração de usuários
• Papéis e atribuições
• Utilização da base local
• Integração com bases externas
• Suporte

Processo de Suporte e Manutenção
• Principais atividades envolvidas
• Processo de atualização do Cisco FTD e Cisco Firepower Management
• Procedimentos de backup e restore

Atividades de laboratório
• Lab 1: Acesso ao laboratório
• Lab 2: Acesso, login e navegação pelo Cisco Firepower Management GUI

- Lab 3: Gerenciamento dos equipamentos (Cisco FTD)
- Lab 4: Configuração Inicial
- Lab 5: Configuração de NAT
- Lab 6: Configuração da descoberta da rede (Network Discovery)
- Lab 7: Configuração das regras de acesso (Access Control Policy)
- Lab 8: Configuração para proteção anti-malware (AMP)
- Lab 9: Configuração de NGIPS no Cisco FTD
- Lab 10: Análise detalhada das informações
- Lab 11: Administração do sistema
- Lab 12: Processo de suporte e manutenção