

FTDNGFW (TELECON O&M CISCO FTD NGFW & NGIPS)

7.0

Objetivo

Podemos destacar os seguintes objetivos desse treinamento: • 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; • Procedimentos de suporte para o FTD.

Público Alvo

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

Pré-Requisitos

Para maior aproveitamento é recomendado que o aluno possua: • Conhecimentos básicos em segurança; • 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

- Arquitetura da Solução
- Portfólio de Produtos
- Cisco Firepower Appliances & FXOS
- Cisco Firepower Management Center & Orchestrators
- Cisco Firepower Device Manager
- Diferenciais da Solução
- Integração com outras soluções (PxGrid)
- 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
- Recomendações e Procedimentos Para Upgrade

Instalação e configuração inicial do Cisco FTD

- Procedimentos e Cuidados para Instalação
- Cenários e Opções para configuração
- Procedimentos para instalação
- Configuração inicial
- Solução Firewall Transparent e Routed
- Integração com o Cisco Firepower Management

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 de Rotas e Roteamento Dinâmico

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
- Configuração de Objetos e Utilização nas Regras
- Estrutura e design das políticas e regras
- Conceitos de controle de regras tipo “Bypass”
- Conceitos das regras de acesso e sua aplicação no Cisco FTD
- Configuração e aplicação das políticas de acesso
- Regras de Configuração: Usuários e Grupos
- Regras de Configuração: Inspeção Protocolo SSL
- Regras de Configuração: Inspeção de Aplicativos
- Regras de Configuração: Inspeção de URLs

Utilização do Security Intelligence

- Conceitos de Security Intelligence
- Cisco Talos & Listas de Reputação
- Utilização do SI: URLs
- Utilização do SI: Domínios
- Utilização do SI: IP´s
- Utilização do SI: Filtros Customizados
- Cisco SI: White List & Black Lists
- 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
- Filtragem de Arquivos
- Monitoramento e Suporte
- 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

Cisco FTD & Soluções em HA

- Arquitetura FTD para HA
- Solução: Cisco FTD Failover (Hot & Standby)

- Solução: Múltiplas Instâncias
- Solução: FTD Cluster
- Solução: FMC HA

Cisco FTD & Soluções em VPN

- Conceitos de VPN
- Aplicações de VPN: Site-to-Site
- Aplicações de VPN: Remote Access-VPN
- Cisco Anyconnect aplicado em VPN
- Configurações de Solução: Site-to-Site
- Configurações de Solução: Remote Access VPN

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

Atividade 1: Acesso LAB Telecon FTD

Recursos Requeridos

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: Configuração de solução VPN Remote Access com Anyconnect

Tarefa 1: Preparação dos requisitos no Cisco FMC

Tarefa 2: Configuração da VPN Remote Access pelo Cisco Firepower Wizard

Tarefa 3: Configuração da política de NAT de exceção para VPN Remote Access

Tarefa 4: Configuração da ACP para permissão de conexões VPN Remote Access

Tarefa 5: Teste e validação da configuração VPN Remote Access

Atividade 13: Administração da Solução Cisco Firepower: Parte 1

Tarefa 1: Agendamento de tarefas (Aplicação de ACP)

Tarefa 2: Automatizando o procedimento "Firepower Recommendations"

Atividade 14: 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 15: Configuração de Alta Disponibilidade do Cisco FTD

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

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

Task 3: Performando testes da solução Cisco FTD HA Failover

Atividade 16: 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