ASANGFW

Telecon O&M Cisco ASA NGFW

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

INTRODUÇÃO

Esse treinamento apresenta os conceitos de segurança aplicados para o produto Cisco ASA Firewall, seguindo as melhores práticas recomendadas pelo fabricante.

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 ASA Firewall utilizando a ferramenta de configuração ASDM (Asa Security Device Manager) e pela linha de comando (Cisco ASA CLI).

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).

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

OBJETIVO DO CURSO

Podemos destacar os seguintes objetivos desse treinamento:
• Descrever os principais recursos da família Cisco ASA 5500-X Next-Generation Firewalls;
• Descrever como implantar a conectividade básica do Cisco ASA e gerenciamento desses dispositivos;
• Proceder a Integração do Cisco ASA em uma Rede de Camada 3;
• Descrever e Implantar os Controles de Acesso do Cisco ASA;
• Descrever e Implantar Regras de NAT;
• Descrever e Implantar Inspeções MPF;
• Descrever e Implantar Inspeções Avançada Camadas 5 a 7;
• Entender e Implantar Soluções VPN Site-to-Site com o Cisco ASA;
• Entender e Implantar Soluções VPN Remote Access com o Cisco ASA;
• Entender e Implantar Soluções VPN de túnel completo Cisco ASA e Cisco AnyConnect;[
• Entender e Implantar Soluções em Alta Disponibilidade da Solução.

PÚBLICO-ALVO

Profissionais que desejam implementar, instalar, configurar, operar e dar suporte ao produto.

PRÉ-REQUISITOS

Recomendamos que os alunos possuam as seguintes habilidades e conhecimentos prévios:

• Conhecimentos básicos em redes IP;

• Conhecimentos básicos em segurança de redes.

CONTEÚDO PROGRAMÁTICO

Introdução ao treinamento

Apresentação dos objetivos

Metas e objetivos a serem alcançados

Introdução ao Cisco ASA Firewall

Tecnologias empregadas no Cisco ASA

Tecnologias de firewall

Apresentação dos Recursos do Cisco ASA

Apresentação das opções em modelos de dispositivos

Arquitetura Cisco ASA

Opções de licenciamento do Cisco ASA

Cisco ASA e Integração da Solução em Uma Rede

Preparando o Cisco ASA para integração de rede

Gerenciando o processo de inicialização do Cisco ASA

Gerenciando o Cisco ASA utilizando CLI (Linha de Comando)

Gerenciando o Cisco ASA utilizando Cisco ASDM

Apresentação dos recursos do Cisco ASDM

Descrevendo o processo de atualização do Cisco ASA

Realizando as configurações básicas do Cisco ASA

Gerenciando os níveis de segurança do Cisco ASA

Configurando e Verificando Parâmetros Básicos em Conectividade

Configurando e Verificando Configurações em VLANs de Interface

Configurando uma rota padrão (Default Gateway)

Configurando e Verificando o Serviço DHCP do Cisco ASA

Solução de problemas de conectividade básica

Procedendo a Integração Junto a Rede

Configurando recursos em NAT do Cisco ASA

Configurando Nat: Objeto (Auto) NAT

Configurando Nat: Manual Nat

Ajustando e solucionando problemas em NAT no Cisco ASA

Configuração para Controle de Acesso do Cisco ASA

Entendendo a Tabela de conexão e tabela de host local

Configurando e Verificando a aplicação de ACLs em Interfaces

Configurando e verificando ACLs globais

Configurando e Verificando Grupos de Objetos

Configurando e Verificando Servidores Públicos

Solução de problemas de ACLs

Configurando recursos de roteamento do Cisco ASA

Emprego do Roteamento Estático

Emprego do Roteamento Dinâmico

Exemplos: Roteamento Dinâmico com EIGRP e OSPF

Entendendo Suporte a Multicast

Serviços de Inspeção do Cisco ASA

Definindo o Cisco ASA MPF

Visão geral do Cisco ASA MPF

Configurando e Verificando as Políticas em Camada 3 e 4

Configurando e Verificando uma Política para Gerenciamento de Tráfego

Configurando as inspeções de aplicativos avançados do Cisco ASA

Visão geral do controle de política em camada 5 à camada 7

Configuração e verificação de inspeção HTTP

Configurando e Verificando a Inspeção de FTP

Suportando Outros Aplicativos em Camada 5 a Camada 7

Solução de problemas de inspeção em camada de aplicativo

Componentes comuns em VPN do Cisco ASA

Visão geral da Arquitetura em VPN

Definição e Conceitos em VPN

Emprego em Tipos de VPN

Apresentação dos Componentes VPN

Implementação de perfis, políticas de grupo e políticas de usuário em VPN

Configuração de política de VPN Cisco ASA

Perfis de conexão do Cisco ASA

Políticas de grupo do Cisco ASA

Cisco ASA VPN & AAA

Atributos de usuário do Cisco ASA

Métodos de controle de acesso em VPN

Implementando serviços de PKI

Utilizando Serviços em PKI no Cisco ASA

Provisionando certificados no Cisco ASA

Integração com Servidores/CA

Implantando autenticação utilizando certificado digital

Operações Utilizando Cisco SCEP

Habilitar autenticação de certificado no perfil de conexão

Configurando Mapeamentos do Perfil de Certificado para Conexão

Solução Cisco Clientless VPN

Apresentando Clientless SSL VPN

Casos de emprego da VPN SSL Clientless

Métodos de acesso a recursos VPN Clientless

Configuração de sessão SSL e gerenciamento de chaves

Autenticação de servidor SSL

Autenticação de cliente SSL

Proteção de transmissão SSL

Implantando Cisco VPN SSL Clientless no Cisco ASA

Autenticação de servidor em VPN SSL

Autenticação do lado do cliente em VPN SSL

Filtros e controles de URL VPN SSL

Controle de acesso básico Portal SSL

Desativando a reescrita de conteúdo

Tarefas básicas de configuração em Portal VPN SSL

Cenário de configuração Portal VPN SSL

Configurando Cisco Portal VPN SSL

Solução de problemas com Portal VPN SSL

Implantação do Controle de Acesso em Aplicativo em Portal SSL VPN

Visão geral do acesso ao aplicativo em Portal VPN SSL

Plug-ins de aplicativos

Configurando Plug-ins de Aplicativos

Verificar plug-ins de aplicativo em Portal VPN SSL

Solução de problemas de plug-ins de aplicativos

Emprego de Túneis Inteligentes (Smart Tunnel) Cisco ASA

Configurando Túneis Inteligentes (Smart Tunnel)

Verificando Túneis Inteligentes (Smart Tunnel)

Resolução de problemas

Implementando autenticação e autorização do lado do cliente em Clientless SSL VPN

Opções de autenticação do lado do cliente

Autenticação e autorização do lado do cliente usando servidor AAA

Autenticação dupla do lado do cliente usando servidores AAA

Solução de problemas

Emprego de Soluções VPN Cisco AnyConnect

Implantando Acesso VPN com Cisco AnyConnect

Autenticação de clientes e provisionamento do cliente Anyconnect

Atribuição de endereço IP ao Cliente Anycoonect

Configuração da política “Split Tunneling”

Cenários Exemplo de Configuração

Tarefas de configuração

Como Ativar Cisco AnyConnect SSL VPNs

Definição do pool de endereços IP

Configurar o NAT de identidade

Configurar Política de Grupo

Configurar Perfil de Conexão

Monitorar Conexões de VPN Cisco AnyConnect

Implantando Cisco AnyConnect Avançado

Componentes da solução Cisco AnyConnect VPN

Visão geral do DTLS

Túneis DTLS e TLS paralelos

Configurar DTLS

Verificar DTLS

Gerenciamento de configuração do cliente Cisco AnyConnect (Profiles)

Gerenciando atualização do software Cisco AnyConnect pelo Cisco ASA

Opções de integração do sistema operacional Cisco AnyConnect Client

Implantando a detecção de rede confiável Cisco AnyConnect

Emprego do Cisco AnyConnect Start Before Logon

Implantando autenticação e autorização avançadas em VPNs Cisco AnyConnect

Autenticação de servidor baseada em certificado

Métodos para revogar credenciais

Habilitar autenticação baseada em certificado

Habilitar autenticação de dois fatores

Visão geral da autorização local

Procedimento de configuração de autorização local

Configurar autorização local

Verifique a autorização local

Cenário de Autorização Externa

Configurar autorização usando LDAP / AD

Verificar autorização externa

Resolução de problemas

Implantação de VPNs Cisco AnyConnect com IPsec / IKEv2

Suporte Cisco AnyConnect para IKEv2

Internet Key Exchange v1 e v2

Tornando o IPsec o protocolo principal

Procedimento de configuração do IKEv2

Cisco ASA & Alta disponibilidade

Configurando recursos de redundância de interface

Configurando e Verificando Interfaces com EtherChannel

Configurando e Verificando Interfaces Redundantes

Resolução de problemas de EtherChannel e interfaces redundantes

Configurando Cisco ASA Faiolver

Visão geral do Cisco ASA failover

Opções de configuração do Cisco ASA Failover

Configurando e verificando Cisco ASA Failover

Ajustando e gerenciando Cisco ASA Failover

Solução de problemas em Cisco ASA Failover

Cisco ASA e Contextos de Segurança

Utilizando o Modo de Contexto Múltiplo

Configurando contextos de segurança

Verificando e Gerenciando Contextos de Segurança

Configurando e Verificando o Gerenciamento de Recursos

Solução de problemas em contextos de segurança

Labs

Lab 1: Acessando o ambiente de laboratório remoto

Lab 2: Configuração Inicial do Cisco ASA

Lab 3: Configurando Cisco ASA NAT

Lab 4: Configurando recursos básicos para controle de acesso

Lab 5: Configurando MPF, Inspeções Básicas e QoS

Lab 6: Configurando inspeções de aplicativos com MPF

Lab 7: Implantando Cisco ASA VPN SSL Clientless

Lab 8: Configurando o controle de acesso ao aplicativo para VPN SSL Clientless

Lab 9: Implantando autenticação externa e autorização para VPNs SSL Clientless

Lab 10: Implantando Cisco ASA AnyConnect SSL VPN básica

Lab 11: Configurando autenticação avançada para Cisco AnyConnect SSL VPNs

Lab 12: Configurando Cisco ASA VPN Cisco AnyConnect IPsec / IKEv2

Lab 13: Configurando Cisco ASA Failover

\n