



Securing Networks with ASA Advanced

Objectifs

Après avoir suivi le cours, les stagiaires seront capables de :

- Configurer les politiques de NAT en fonction du trafic
- Décrire la politique modulaire de firewalling
- Décrire l'inspection avancée des protocoles applicatifs
- Configurer des VLAN
- Configurer un protocole de routage
- Comprendre les composants et les fonctionnalités d'IPsec et comprendre comment les certificats digitaux sont utilisés
- Configurer un tunnel Site à site en utilisant des certificats digitaux
- Configurer le client VPN Cisco en utilisant des certificats digitaux
- Configurer la solution de sécurité en tant que client VPN
- Configurer la solution de sécurité ASA 5505 comme VPN client hardware
- Configurer de la QOS pour le trafic VPN
- Configurer le WEBVPN sur la solution de sécurité
- Identifier les fonctionnalités du client SSL
- Configurer un VPN SSL en utilisant le client Cisco AnyConnect
- Décrire le Cisco Secure Desktop
- Configurer le Cisco Secure Desktop et le DAP
- Configurer le module CSC pour le filtrage et l'inspection du trafic

SNA

3250 € HT
Version : 1.0
5 jours

A qui s'adresse ce cours ?

Aux clients Cisco® chargés de l'implémentation et de la gestion des dispositifs de sécurité ASA.

Aux ingénieurs système Cisco® qui interviennent suite à la vente de dispositifs de sécurité ASA.

Pré-requis

Etre certifié CCNA ou avoir un niveau équivalent
Posséder des bases sur les environnements Microsoft Windows
Etre familiarisé avec les notions et concepts de sécurités réseaux

Contenu du stage

- 1. Configuration et vérification du NAT, du routage dynamique, et du switching sur les solutions de sécurité.**
 - 1.1. Configurer les VLAN en utilisant ASDM
 - 1.2. Configurer les protocoles de routage dynamique et les redistributions de route en utilisant ASDM
 - 1.3. Configurer les politiques de NAT en utilisant ASDM

Pour plus d'informations : info@learneo.com ou 01 53 20 37 00

CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and Networking Academy are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this Web site are the property of their respective owners.



2. Configuration et vérification de l'inspection des protocoles applicatifs et la politique modulaire pour les solutions de sécurité.

- 2.1. Décrire les capacités de traitement des protocoles applicatifs sur la solution de sécurité
- 2.2. Configurer et vérifier l'inspection des protocoles applicatifs en utilisant ASDM
- 2.3. Configurer et vérifier la politique modulaire en utilisant ASDM

3. Configurer une connexion sécurisée en utilisant des VPN IPsec

- 3.1. Décrire les points clés et les capacités des certificats digitaux
- 3.2. Décrire comment utiliser l'inscription des certificats digitaux avec la solution de sécurité et le client VPN Cisco
- 3.3. Configurer les VPN accès distant avec des certificats digitaux en utilisant ASDM
- 3.4. Configurer les clients VPN IPsec avec des certificats digitaux en utilisant ASDM
- 3.5. Configurer un VPN site à site avec des certificats digitaux en utilisant ASDM
- 3.6. Configurer un VPN accès distant avancé en utilisant ASDM
- 3.7. Configurer un ASA 5505 comme client de l'accès distant en utilisant ASDM
- 3.8. Configurer de la QOS pour le trafic passant dans un tunnel en utilisant ASDM

4. Configurer et valider une connexion sécurisée en utilisant du VPN SSL

- 4.1. Décrire les fonctionnalités et les capacités d'un VPN SSL
- 4.2. Configurer et vérifier l'autorité de certification locale en utilisant ASDM
- 4.3. Configurer et vérifier des smart tunnels des plug-ins et des liens en utilisant ASDM
- 4.4. Configurer et vérifier la redirection de port en utilisant ASDM
- 4.5. Configurer la solution de sécurité pour l'accès client VPN SSL
- 4.6. Configurer le client AnyConnect
- 4.7. Configurer le Cisco Secure Desktop en utilisant ASDM
- 4.8. Configurer le Dynamic Access Policies en utilisant ASDM

5. Configurer et valider les modules SSM

- 5.1. Expliquer la fonction d'un module AIP-SSM et CSC-SSM dans un réseau
- 5.2. Configurer et valider le module AIP-SSM
- 5.3. Configurer et valider le module CSC-SSM

Déroulement du stage

	Jour 1	Jour 2	Jour 3	Jour 4	Jour 5
MATIN	NAT Politique de firewalling modulaire	Protocole de routage et Certificat avec IPSEC	VPN accès distant	VPN SSL	Cisco Secure Desktop et DAP
Déjeuner					
APRES-MIDI	Inspection avancé et VLAN	VPN Site à site Client VPN Cisco	VPN acces distant avec le ASA 5505 QOS pour les VPNs IPsec	VPN SSL Cisco Secure Desktop	AIP-SSM CSC-SSM

Pour plus d'informations : info@learneo.com ou 01 53 20 37 00

CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and Networking Academy are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

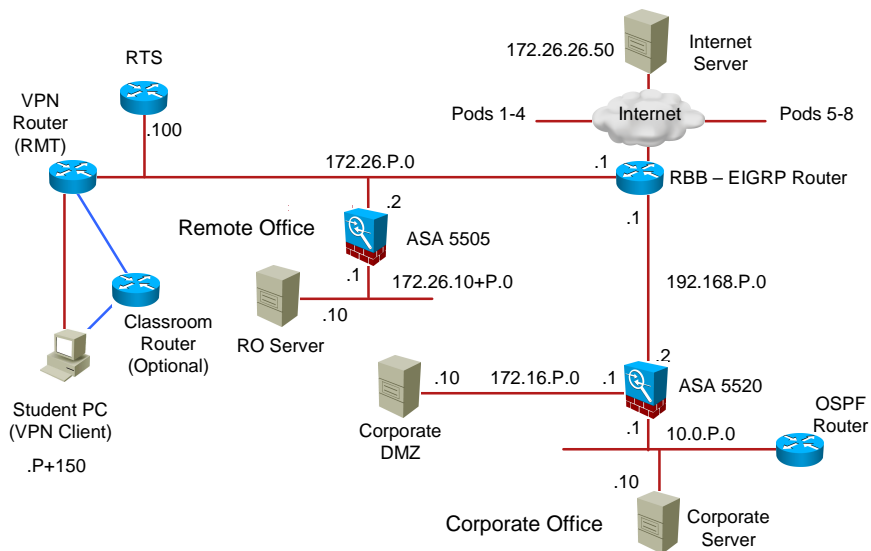
All other trademarks mentioned in this Web site are the property of their respective owners.



Laboratoires pratiques

- Lab 1-1: Implementing Advanced NAT
- Lab 2-1: Configuring Advanced Protocol Inspection
- Lab 3-1: Dynamic Routing with EIGRP and OSPF
- Lab 4-1: Site-to-Site with Digital Certificates
- Lab 4-2: Remote Access with Digital Certificates
- Lab 4-3: Cisco ASA 5505 Easy VPN Hardware Client
- Lab 5-1: Clientless SSL VPNs
- Lab 5-2: SSL VPNs with Cisco AnyConnect Client
- Lab 5-3: Cisco Secure Desktop and Dynamic Access Policy
- Lab 6-1: Initializing the Cisco AIP-SSM

Lab Topology



© 2008 Cisco Systems, Inc. All rights reserved.

SNAA v1.0-3

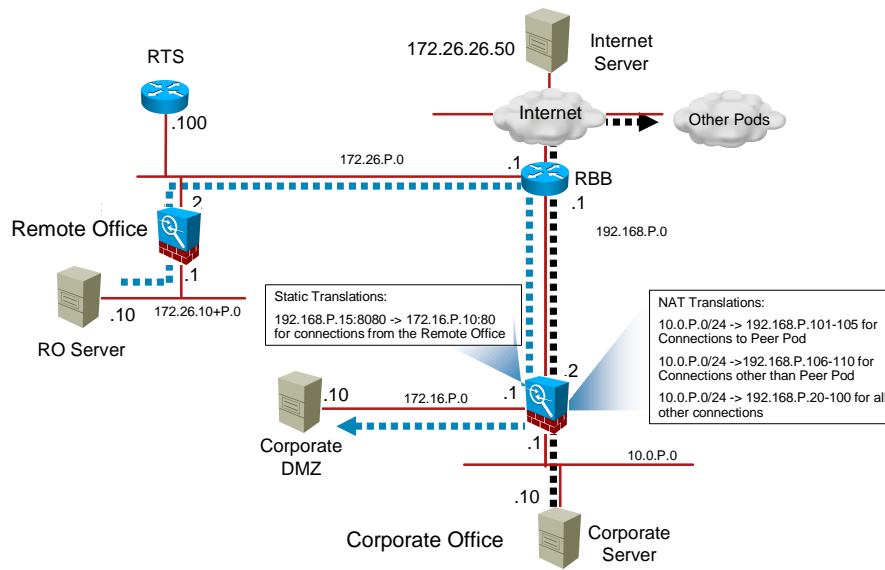
Pour plus d'informations : info@learneo.com ou 01 53 20 37 00

CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and Networking Academy are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this Web site are the property of their respective owners.



Lab 1-1 Visual



© 2008 Cisco Systems, Inc. All rights reserved.

SNA4 v1.0-4

Pour plus d'informations : info@learneo.com ou 01 53 20 37 00

CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and Networking Academy are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this Web site are the property of their respective owners.