# Table of Contents

Preface ........................................................................................................................................1

CVD Navigator .............................................................................................................................2
  Use Cases ............................................................................................................................. 2
  Scope ................................................................................................................................. 2
  Proficiency ........................................................................................................................ 2

Introduction .................................................................................................................................3
  Technology Use Case ............................................................................................................ 3
    Use Case: Teleworker with Wired Ethernet Devices ....................................................... 3
  Design Overview ................................................................................................................... 3

Deployment Details .................................................................................................................. 5
  Configuring Cisco Secure ACS for Teleworker VPN ....................................................... 5
  Configuring RAVPN Cisco ASA for Teleworker VPN ..................................................... 9
  Configuring Teleworker Cisco ASA 5505 Endpoints ..................................................... 20

Appendix A: Product List ...........................................................................................................26

Appendix B: Tested Topology ..................................................................................................27

Appendix C: Configuration Files ..............................................................................................29
    VPN-ASA5525X ............................................................................................................... 29
    ASA-5505 ....................................................................................................................... 43

Appendix D: Changes ...............................................................................................................47
Cisco Validated Designs (CVDs) present systems that are based on common use cases or engineering priorities. CVDs incorporate a broad set of technologies, features, and applications that address customer needs. Cisco engineers have comprehensively tested and documented each design in order to ensure faster, more reliable, and fully predictable deployment.

CVDs include two guide types that provide tested design details:

- **Technology design guides** provide deployment details, information about validated products and software, and best practices for specific types of technology.

- **Solution design guides** integrate existing CVDs but also include product features and functionality across Cisco products and sometimes include information about third-party integration.

Both CVD types provide a tested starting point for Cisco partners or customers to begin designing and deploying systems.

**CVD Foundation Series**

This CVD Foundation guide is a part of the August 2014 Series. As Cisco develops a CVD Foundation series, the guides themselves are tested together, in the same network lab. This approach assures that the guides in a series are fully compatible with one another. Each series describes a lab-validated, complete system.

The CVD Foundation series incorporates wired and wireless LAN, WAN, data center, security, and network management technologies. Using the CVD Foundation simplifies system integration, allowing you to select solutions that solve an organization’s problems—without worrying about the technical complexity.

To ensure the compatibility of designs in the CVD Foundation, you should use guides that belong to the same release. For the most recent CVD Foundation guides, please visit the CVD Foundation web site.

**Comments and Questions**

If you would like to comment on a guide or ask questions, please use the feedback form.
The CVD Navigator helps you determine the applicability of this guide by summarizing its key elements: the use cases, the scope or breadth of the technology covered, the proficiency or experience recommended, and CVDs related to this guide. This section is a quick reference only. For more details, see the Introduction.

**Use Cases**

This guide addresses the following technology use cases:

- **Teleworker with Wired Ethernet Devices**—Teleworkers who need always-on, secure access to networked business services from the remote home office often require telework resources connected with wired Ethernet.

For more information, see the "Use Cases" section in this guide.

**Scope**

This guide covers the following areas of technology and products:

- Remote-site teleworking using the Cisco Adaptive Security Appliance
- Internet edge firewall and VPN termination on Cisco Adaptive Security Appliances

For more information, see the "Design Overview" section in this guide.

**Proficiency**

This guide is for people with the following technical proficiencies—or equivalent experience:

- **CCNA Security**—1 to 3 years installing, monitoring, and troubleshooting network devices to maintain integrity, confidentiality, and availability of data and devices

To view the related CVD guides, click the titles or visit the CVD Foundation web site.
Technology Use Case

Many organizations face increasing need to offer a telecommuter solution to their employees. Employees perceive that commuting and water-cooler chatter are time they spend at work, and renting or buying office space and fixtures, and even deploying network infrastructure to host the work force, adds up to a substantial sum of capital and operating expense.

Providing an office-like work environment at the teleworker’s home requires:

- A phone that is accessible as an extension on the organization’s phone system.
- An unobtrusive, quiet, low-power solution to provide multiple Ethernet connections for one or more IP-phones or other desktop collaboration resources.
- One or more Ethernet connections for computers that access the organization’s network, as well as Ethernet connectivity for other network-connected devices, such as printers and IP video surveillance equipment.

Employees don’t need wireless connectivity at the telework site because all of the telework resources connect with wired Ethernet.

Use Case: Teleworker with Wired Ethernet Devices

Teleworkers require always-on secure access to networked business services from the remote home office. Sometimes employees don’t need wireless connectivity at the telework site because all of the telework resources connect with wired Ethernet.

This design guide enables the following network capabilities:

- Authentication for employees before they can communicate with internal resources and encryption for all information sent and received to the organization’s main location
- Co-residence with the organization’s Internet edge firewall or remote-access VPN setup
- Power over Ethernet (PoE) for voice endpoints at the teleworker location

Design Overview

Cisco Adaptive Security Appliance (ASA) 5505 offers a low-cost option to provide teleworker connectivity to the organization. Cisco ASA 5505 provides secure connectivity for data and collaboration endpoints in a compact, fanless form factor, minimizing noise and space requirements.

The Cisco ASA 5505 teleworker solution integrates at the organization’s Internet edge. The teleworker’s connection terminates at resilient Cisco ASA firewalls at the organization’s Internet edge. This solution is configured on the same ASA firewalls as the remote-access virtual private network (RAVPN) solution. This configuration applies to dedicated and shared-mode RAVPN deployments. Some of the configuration re-uses portions of the RAVPN configuration, although it may be configured to be completely independent of the RAVPN resources. The addition of the head-end’s support for Cisco ASA 5505 teleworker termination does not affect RAVPN connectivity, and the configuration can be applied without the imposition of a service outage.
The Cisco ASA 5505 teleworker solution provides access for endpoint devices, such as laptop and desktop computers, IP phones, printers, and other devices that connect to the network via wired Ethernet connections. Two of the Cisco ASA 5505’s ports provide Power over Ethernet (PoE) to support IP phones, IP video surveillance, and other endpoints without cluttering the teleworker’s office with additional cables and wall-wart power supplies.

The Cisco ASA 5505 teleworker solution offers:

- **Low cost**—With this solution, you get a Cisco ASA 5505, a Cisco IP phone, and the necessary license on the organization’s Internet edge Cisco ASAs.
- **Flexible connectivity**—The Cisco ASA 5505’s integrated Ethernet switch can accommodate multiple endpoint devices, including two interfaces that can provide PoE.
- **Simple deployment**—The Cisco ASA 5505 can be configured quickly with a brief text-file configuration.
- **Security**—Deactivation of the teleworker site’s credentials on the Internet-edge appliance can terminate the teleworker’s connectivity.

Ideally, the Cisco ASA 5505 teleworker device is preconfigured and sent home with the teleworker user. A newly-provisioned or existing desktop IP-phone can be taken home, as well, and registers to the Cisco Call Manager server over the VPN.
Configuration of remote-access connectivity consists of three phases. In the first phase, you configure Cisco Secure ACS to authenticate and authorize teleworker users. In the second phase, you configure your resilient Internet-edge appliance pair to receive VPN connections from teleworkers’ Cisco ASA 5505 appliances. In the third phase, you deploy configuration on the teleworkers’ Cisco ASA 5505 hardware clients.

### Configuring Cisco Secure ACS for Teleworker VPN

1. Create authorization profile
2. Create an authorization rule

This design uses Cisco Secure ACS in conjunction with Microsoft Active Directory for authentication of teleworkers who remotely connect to the enterprise via the Cisco ASA 5505 appliance.

When the Cisco ASA firewall queries the Cisco Secure ACS server (which then proxies the request to the Active Directory database) to determine whether a user’s name and password is valid, Cisco Secure ACS also retrieves other Active Directory attributes, such as group membership. Based on this group membership, Cisco Secure ACS sends back a group policy name to the ASA appliance, along with the success or failure of the login. Cisco ASA uses the group policy name in order to assign the user to the appropriate VPN group policy.
In this process, Active Directory is the primary directory container for user credentials and group membership. Before you begin this process, your Active Directory must have a vpn-teleworker group defined.

<table>
<thead>
<tr>
<th>User name</th>
<th>Active Directory Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN-teleworker-1</td>
<td>cisco.local/Users/vpn-teleworker</td>
</tr>
<tr>
<td>VPN-teleworker-2</td>
<td>cisco.local/Users/vpn-teleworker</td>
</tr>
</tbody>
</table>

**Procedure 1  Create authorization profile**

Create an authorization profile in order to identify teleworker users that belong to the vpn-teleworker group in Active Directory.

**Step 1:** In Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles, click Create.

**Step 2:** In the Name box, enter a name for the authorization profile. (Example: VPN-Teleworker)

**Step 3:** Click the RADIUS Attributes tab, and then in the RADIUS Attribute row, click Select.

**Step 4:** In the RADIUS Dictionary dialog box, pane, select Class, and then click OK.

Next, you must configure the attribute value to match the group policy that you will configure on the Cisco ASA appliance.

**Step 5:** In the Attribute Value box, enter the group policy name, and then click Add. (Example: GroupPolicy_5505)

**Tech Tip**

The group policy name must exactly match the group policy name of the Teleworker5505 connection profile on the ASA appliance, configured later in this document.
Step 6: Click Submit.

Procedure 2 Create an authorization rule


Step 2: In the Name box, enter a rule name. (Example: VPN-Teleworker)


Step 4: In the condition definition box, select the Active Directory group. (Example: cisco.local/Users/vpn-teleworker)
Step 5: Under Results, select the authorization profile, and then click Select. (Example: VPN-Teleworker)

Step 6: Click OK.
Configuring RAVPN Cisco ASA for Teleworker VPN

1. Configure IPsec(IKEv1) connection profile
2. Configure NAT exemption
3. Configure route advertisement

As a rule, the Cisco ASA configuration for Cisco ASA 5505 teleworker VPN is self-contained. A few aspects rely on configuration from the Internet-edge foundation, so you need to have followed the configuration steps for Cisco ASA-based Remote Access VPN in the Remote Access VPN Design Guide.

Procedure 1 Configure IPsec(IKEv1) connection profile

The IPsec connection profile carries the bulk of the configuration that sets the behavior for VPN client connections, so you must apply a number of steps in this procedure to complete the central configuration.

Step 1: Launch the Cisco ASA Security Device Manager.


Step 3: In the right pane under Connection Profiles, click Add.
Step 4: On the Add IPsec Remote Access Connection Profile dialog box, enter the following details. This configuration affects the behavior of the Cisco ASA 5505 teleworker device, as described.

- **Name—**Teleworker5505
  This entry is the name of the VPN group that is reflected in the Cisco ASA 5505 Easy VPN Client configuration.

- **IKE Peer Authentication Pre-Shared Key—**cisco123
  This entry is the group key that must be duplicated in the Cisco ASA 5505 Easy VPN Client configuration.

- **Server Group—**Select **AAA-RADIUS** or **AD**, depending on whether you are using Access Control Service (ACS) or Microsoft Active Directory for user authentication.
  This entry selects the server that authenticates user names and passwords that are presented to open the Easy VPN Client tunnel.

Step 5: On the right side of the **Group Policy** list, click **Manage**.

Step 6: On the Configure Group Policies dialog box, click **Add**.
Step 7: On the Add Internal Group Policy dialog box, select General, and then in the Name box, enter GroupPolicy_5505.

![Add Internal Group Policy dialog box](image)

**Tech Tip**

The Name must exactly match the group policy name of the VPN-Teleworker authorization profile provisioned on the ACS earlier in this document.

Step 8: Expand the options panel by clicking More Options.

![More Options panel](image)

Step 9: Next to Tunneling Protocols, clear Inherit, and then select IPsec IKEv1.

![Tunneling Protocols panel](image)

Step 10: Navigate to Advanced > Split Tunneling, and in the right panel, next to Policy, clear Inherit.
Step 11: Next to **Policy**, in the drop-down list, ensure that **Tunnel All Networks** is selected.

Step 12: Navigate to **Advanced > IPsec(IKEv1) Client**.

Step 13: Next to **Store Password on Client System**, clear **Inherit** and ensure that **Disable** is selected.
Step 14: Navigate to Advanced > IPSec(IKEv1) Client > Hardware Client, and do the following:

- Next to Require Interactive Client Authentication, clear Inherit and ensure that Enable is selected.
- Next to Allow Network Extension Mode, clear Inherit and ensure that Enable is selected.
- Click OK.

Step 15: On the Configure Group Policies dialog box, click OK.

Step 16: On the Add IPSec Remote Access Connection Profile dialog box, and then clear Enable L2TP over IPSec protocol.
Step 17: Navigate to Advanced > General.

Step 18: Under Password Management, select Enable password management, and then click OK.


Step 20: Under Access Interfaces, next to the appliance’s primary outside interface, select Allow Access.

Step 21: Under Connection Profiles, verify that the new Teleworker5505 profile appears, and then click Apply.
**Configure NAT exemption**

The Internet-edge appliances must not apply network address translation (NAT) on traffic between the organization’s private network and the IP-subnet that encompasses teleworkers’ remote addresses. You must configure a policy that prevents the Internet-edge appliance from applying NAT.

Configure a network object for the summary address of the internal network. The network object will be used during the security policy configuration.

**Step 1:** Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**.

**Step 2:** Click on **Add > Network Object**.

**Step 3:** On the Add Network Object dialog box, in the **Name box**, enter a description for the network summary (Example: internal-network).

**Step 4:** In the **Type** list, choose *Network*.

**Step 5:** In the **IP Address** box, enter the address that summarizes all internal networks (Example: 10.4.0.0).

**Step 6:** In the **Netmask** box, enter the internal network summary netmask, and then click **OK** (Example: 255.254.0.0).

**Step 7:** Navigate to **Configuration > Firewall > NAT Rules**, and then click **Add**.

**Step 8:** On the Add NAT Rule dialog box, under **Match Criteria: Original Packet**, in the **Source Address** box, click the ellipsis (...).
Step 9: On the Browse Original Source Address dialog box, expand the IPv4 Network Objects list, double-click internal-network, and then click OK.

![Browse Original Source Address](image)

Step 10: On the Add NAT Rule dialog box, under Match Criteria: Original Packet, in the Destination Address box, click the ellipsis (...).

![Add NAT Rule](image)

Step 11: On the Browse Original Destination Address dialog box, click Add, and then click Network Object.

![Browse Original Destination Address](image)
Step 12: On the Add Network Object dialog box, enter the following values, and then click OK.

- **Name**: 5505-pool
- **Type**: Network
- **IP Address**: 10.4.156.0
- **Netmask**: 255.255.252.0
- **Description**: 5505 Teleworker Subnet

![Add Network Object dialog](image1)

Step 13: On the Browse Original Destination Address dialog box, expand the IPv4 Network Objects list, double-click 5505-pool, and then click OK.

![Browse Original Destination Address](image2)
Step 14: Under Options, ensure that Enable Rule and Disable Proxy ARP on egress interface are selected and that the indicated direction is Both, and then click OK.

Step 15: Review the configuration, and then click Apply.

**Procedure 3 Configure route advertisement**

The Internet-edge appliances must advertise the teleworker sites’ networks to the internal network. RAVPN address pools are advertised as host routes by reverse route injection (RRI) and summarized by the Internet-edge appliance. Teleworker subnets are advertised by RRI, as well, but without summarization; the teleworker subnets remain intact as eight-number (/29) subnets advertised to the rest of the network.

Step 2: Select the crypto map listed under the primary outside interface, and then click **Edit**.

Step 3: Click the **Tunnel Policy (Crypto Map) - Advanced** tab.

Step 4: Select **Enable Reverse Route Injection**, and then click **OK**.

Step 5: On the Crypto Maps pane, click **Apply**.
Configuring Teleworker Cisco ASA 5505 Endpoints

1. Configure inside VLAN and switch ports
2. Define global device configuration
3. Configure outside VLAN and switch port
4. Configure Cisco ASA 5505 DHCP server
5. Configure Cisco ASA 5505 Easy VPN client
6. Initiate VPN connection
7. Verify VPN connection

Each teleworker’s Cisco ASA 5505 endpoint must be configured to connect to your resilient Internet-edge appliance. Because this configuration is likely to be deployed on multiple devices, the configuration is shown only in the command-line interface to streamline deployment. All Cisco ASA 5505 teleworker sites connect using Network Extension Mode, which allows teleworker-site endpoints to connect freely to the organization’s LAN. Connecting in Network Extension Mode is particularly critical for endpoints, such as IP phones and video surveillance cameras, which might be susceptible to NAT’s modification of data traffic.

Each site must use a unique inside-IP subnet. Otherwise, all configuration is identical between sites. To avoid conflicting address assignments, Cisco recommends that you maintain a spreadsheet of subnet assignments for the various users that will be issued Cisco ASA 5505 telecommuter equipment.

<table>
<thead>
<tr>
<th>User name</th>
<th>Subnet</th>
<th>ASA 5505 LAN address</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN-teleworker-1</td>
<td>10.4.156.0/29</td>
<td>10.4.156.1</td>
<td>TS01-ASA5505</td>
</tr>
<tr>
<td>VPN-teleworker-2</td>
<td>10.4.156.8/29</td>
<td>10.4.156.9</td>
<td>TS02-ASA5505</td>
</tr>
</tbody>
</table>

Procedure 1 Configure inside VLAN and switch ports

Each Cisco ASA 5505 teleworker site needs a unique inside subnet, which you should track in a spreadsheet, as recommended in the introduction of this section.

Step 1: Configure the VLAN 1 interface for the teleworker site’s LAN.

```
interface Vlan1
  nameif inside
  security-level 100
  ip address 10.4.156.1 255.255.255.248
```
Step 2: Associate the Cisco ASA 5505’s Ethernet 0/1 through Ethernet 0/7 interfaces with VLAN 1, and instruct the teleworker to connect PoE-enabled devices to the Ethernet 0/6 and 0/7 ports.

```bash
interface Ethernet0/1
  switchport access vlan 1
  no shutdown
...
interface Ethernet0/7
  switchport access vlan 1
  no shutdown
```

**Procedure 2** Define global device configuration

**Step 1:** Configure the Cisco ASA 5055’s hostname and domain name.

```bash
hostname TS01-ASA5505
domain-name cisco.local
```

**Step 2:** Define a local administrative username.

```bash
username admin password cisco123 privilege 15
```

**Step 3:** Set the enable password.

```bash
enable password cisco123
```

**Step 4:** Define the management configuration.

```bash
http server enable
http 10.0.0.0 255.0.0.0 inside
ssh 10.0.0.0 255.0.0.0 inside
management-access inside
```

**Step 5:** If you are using centralized AAA, define authentication servers for management access.

```bash
aaa-server AAA-SERVERS protocol tacacs+
aaa-server AAA-SERVERS (inside) host 10.48.48.15
  key SecretKey
aaa authentication http console AAA-SERVERS LOCAL
aaa authentication ssh console AAA-SERVERS LOCAL
```

**Procedure 3** Configure outside VLAN and switch port

**Step 1:** Configure a VLAN interface to receive an IP address via DHCP from the teleworker’s Internet gateway device.

```bash
interface Vlan2
  nameif outside
  security-level 0
  ip address dhcp setroute
```
Step 2: Associate the Cisco ASA 5505’s Ethernet 0/0 interface with VLAN 2, and instruct the teleworker to connect Ethernet 0/0 to their Internet gateway device.

```
interface Ethernet0/0
switchport access vlan 2
no shutdown
```

**Procedure 4** Configure Cisco ASA 5505 DHCP server

The Cisco ASA 5505 must be configured to provide IP-addresses for the teleworker endpoints, such as computers, phones, printers, and video surveillance devices. Each site must use a unique subnet, which should be tracked in a spreadsheet, as recommended in the introduction of this section.

**Step 1:** Define the DHCP scope address range. The DHCP scope must be in the same subnet as the inside (VLAN 1) interface.
```
dhcpd address 10.4.156.2-10.4.156.6 inside
```

**Step 2:** Configure the DNS and domain-name values that will be distributed to clients.
```
dhcpd dns 10.4.48.10 interface inside
dhcpd domain cisco.local interface inside
```

**Step 3:** Define DHCP option 150 to provide the Cisco Unified Call Manager Server address for Cisco IP phones.
```
dhcpd option 150 ip 10.4.48.120
```

**Step 4:** Enable the DHCP scope.
```
dhcpd enable inside
```

**Procedure 5** Configure Cisco ASA 5505 Easy VPN client

Cisco ASA 5505 uses Easy VPN network-extension mode to negotiate the VPN connectivity to the Internet-edge Cisco ASA Remote Access server.

**Step 1:** Apply the Easy VPN client configuration for the remote Cisco ASA 5505: The vpngroup and password values must match the IPsec Remote Access Connection Profile that you configured on the Internet-edge appliance.
```
vpnclient server 172.16.130.122
```

**Step 2:** Set network-extension mode:
```
vpnclient mode network-extension-mode
```

**Step 3:** Define the Easy VPN client connection attributes. The vpngroup and password values must match the IPsec Remote Access Connection Profile that you configured on the Internet-edge appliance.
```
vpnclient vpngroup Teleworker5505 password cisco123
```

**Step 4:** Enable the Cisco ASA 5505’s Easy VPN client:
```
vpnclient enable
```
Initiate VPN connection

The teleworker must manually initiate their VPN connection; when the user employs a web browser to access web content on your internal network, Cisco ASA 5505 intercepts the connection and provides an interactive login prompt.

Tech Tip

Until the Easy VPN tunnel is established, DNS queries from clients behind the appliance will time-out. With the tunnel down, the clients cannot reach the DNS server. To avoid this time delay, you can directly access the Easy VPN connection status web page using an IP address: https://10.4.156.1:1443/netaccess/connstatus.html.

It is convenient to set the web browser home page to the Easy VPN connection status web page.

Step 1: Using a web browser navigate to the Easy VPN connection status web page. You can also navigate to any internal web site. (Example: 10.4.48.10)

https://[ASA 5505 LAN Address]:443/netaccess/connstatus.html

Example

https://10.4.156.1:443/netaccess/connstatus.html

Step 2: You will be redirected to an Easy VPN Connection Status web page.

Step 3: Click Connect Now.

Step 4: Enter the Username. (Example: vpn-teleworker-1)
Step 5: Enter the **Password**. (Example: c1sco123)

Step 6: Enter the **Domain**. (Example: *leave blank*)

The VPN connection is negotiated with the provided username and password, and the requested web page is rendered.

---

**Tech Tip**

The IP Phone connected to Cisco ASA 5505 can't place or receive calls if the user’s VPN connection is not active.

In the event that a teleworker’s VPN access must be revoked, the authentication server should deny the teleworker’s access.
Procedure 7  
Verify VPN connection

You can check the status of the Easy VPN connection from Cisco ASA 5505.

Step 1: Using a web browser, navigate to the ASA 5505 appliance’s Easy VPN connection status web page.  
(Example: https://10.4.156.1:1443/netaccess/connstatus.html)

The Easy VPN connection may also be monitored from the RA VPN ASA appliance.


Step 3: From the Filter By: pull down menus, select IPsec(IKE v1) Remote Access and select -- All Sessions --.
## Appendix A: Product List

### Remote-Site

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Product Description</th>
<th>Part Numbers</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Site Appliance</td>
<td>Cisco ASA 5505 Firewall Edition Bundle security appliance</td>
<td>ASA5505-BUN-K9</td>
<td>ASA 9.1(5)</td>
</tr>
</tbody>
</table>

### Internet Edge

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Product Description</th>
<th>Part Numbers</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>Cisco ASA 5545-X IPS Edition - security appliance</td>
<td>ASA5545-IPS-K9</td>
<td>ASA 9.1(5)</td>
</tr>
<tr>
<td></td>
<td>Cisco ASA 5515-X IPS Edition - security appliance</td>
<td>ASA5515-IPS-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco ASA 5512-X IPS Edition - security appliance</td>
<td>ASA5512-IPS-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco ASA 5512-X Security Plus license</td>
<td>ASA5512-SEC-PL</td>
<td></td>
</tr>
<tr>
<td>Firewall Management</td>
<td>ASDM</td>
<td></td>
<td>7.1(6)</td>
</tr>
<tr>
<td>RA VPN Firewall</td>
<td>Cisco ASA 5545-X Firewall Edition - security appliance</td>
<td>ASA5545-K9</td>
<td>ASA 9.1(5)</td>
</tr>
<tr>
<td></td>
<td>Cisco ASA 5525-X Firewall Edition - security appliance</td>
<td>ASA5525-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco ASA 5515-X Firewall Edition - security appliance</td>
<td>ASA5515-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco ASA 5512-X Firewall Edition - security appliance</td>
<td>ASA5512-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco ASA 5512-X Security Plus license</td>
<td>ASA5512-SEC-PL</td>
<td></td>
</tr>
<tr>
<td>Firewall Management</td>
<td>ASDM</td>
<td></td>
<td>7.1(6)</td>
</tr>
</tbody>
</table>

### Access Control

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Product Description</th>
<th>Part Numbers</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Services</td>
<td>ACS 5.5 VMware Software And Base License</td>
<td>CSACS-5.5-VM-K9</td>
<td>5.5 with Cumulative Patch 5.5.0.46.2 feature set</td>
</tr>
</tbody>
</table>
Appendix B: Tested Topology

Figure 2 - Cisco ASA 5505 physical topology
Figure 3 - Cisco ASA 5505 logical topology

Figure showing the logical topology of Cisco ASA 5505 with various network elements and connections.

(Appendix B: Tested Topology)
VPN-ASA5525X

ASA Version 9.1(5)
!
hostname VPN-ASA5525X
domain-name cisco.local
enable password 8Ry2YjIyt7RRXU24 encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
names
ip local pool RA-pool 10.4.28.1-10.4.31.254 mask 255.255.252.0
!
interface GigabitEthernet0/0
  nameif inside
  security-level 100
  ip address 10.4.24.24 255.255.255.224 standby 10.4.24.23
  ospf message-digest-key 1 md5 *****
  ospf authentication message-digest
  authentication key eigrp 100 ***** key-id 1
  authentication mode eigrp 100 md5
  summary-address eigrp 100 10.4.28.0 255.255.252.0 5
!
interface GigabitEthernet0/1
  shutdown
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/2
  description LAN/STATE Failover Interface
  !
interface GigabitEthernet0/3
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/3.16
  vlan 16
  nameif outside-16
  security-level 0
  ip address 172.16.130.122 255.255.255.0 standby 172.16.130.121
!
interface GigabitEthernet0/3.17
  vlan 17
  nameif outside-17
  security-level 0
  ip address 172.17.130.122 255.255.255.0 standby 172.17.130.121
!
interface GigabitEthernet0/4
  shutdown
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/5
  shutdown
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/6
  shutdown
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/7
  shutdown
  no nameif
  no security-level
  no ip address
!
interface Management0/0
  management-only
  shutdown
  no nameif
  no security-level
  no ip address
!
ftp mode passive
clock timezone PST -8
clock summer-time PDT recurring
dns domain-lookup inside
dns server-group DefaultDNS
domain-name cisco.local
same-security-traffic permit intra-interface
object network Gateway
  host 10.4.24.1
object network NETWORK_OBJ_10.4.28.0_22
  subnet 10.4.28.0 255.255.255.0
object network internal-network
  subnet 10.4.0.0 255.255.0.0
object network 5505-Pool
  subnet 10.4.156.0 255.255.252.0
description 5505 Teleworker Subnet
access-list ALL_BUT_DEFAULT standard deny host 0.0.0.0
access-list ALL_BUT_DEFAULT standard permit any4
access-list RA_PartnerACL remark Partners can access this internal host only!
access-list RA_PartnerACL standard permit host 10.4.48.35
access-list RA_SplitTunnelACL remark Internal Networks
access-list RA_SplitTunnelACL standard permit 10.4.0.0 255.254.0.0
access-list RA_SplitTunnelACL remark DMZ Networks
access-list RA_SplitTunnelACL standard permit 192.168.16.0 255.255.248.0
pager lines 24
logging enable
logging timestamp
logging buffered informational
mtu inside 1500
mtu outside-16 1500
mtu outside-17 1500
failover
failover lan unit secondary
failover lan interface failover GigabitEthernet0/2
failover polltime unit msec 200 holdtime msec 800
failover polltime interface msec 500 holdtime 5
failover key *****
failover replication http
failover link failover GigabitEthernet0/2
failover interface ip failover 10.4.24.97 255.255.255.248 standby 10.4.24.98
monitor-interface outside-16
monitor-interface outside-17
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-716.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
nat (any,any) source static internal-network internal-network destination static 5505-Pool 5505-Pool no-proxy-arp
!
router eigrp 100
no auto-summary
distribute-list ALL_BUT_DEFAULT out
network 10.4.0.0 255.254.0.0
passive-interface default
no passive-interface inside
redistribute static

route outside-16 0.0.0.0 0.0.0.0 172.16.130.126 1 track 1
distribute-list ALL_BUT_DEFAULT out
network 10.4.0.0 255.254.0.0
passive-interface default
no passive-interface inside
redistribute static

route outside-17 0.0.0.0 0.0.0.0 172.17.130.126 50
distribute-list ALL_BUT_DEFAULT out
network 10.4.0.0 255.254.0.0
passive-interface default
no passive-interface inside
redistribute static

route outside-16 172.18.1.1 255.255.255.255 172.16.130.126 1
distribute-list ALL_BUT_DEFAULT out
network 10.4.0.0 255.254.0.0
passive-interface default
no passive-interface inside
redistribute static

route inside 0.0.0.0 0.0.0.0 10.4.24.1 tunneled
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
aaa-server AAA-SERVER protocol tacacs+

aaa-server AAA-SERVER (inside) host 10.4.48.15
    key *****

aaa-server AD protocol nt
aaa-server AD (inside) host 10.4.48.10

    nt-auth-domain-controller AD-1
    user-identity default-domain LOCAL
    aaa authentication enable console AAA-SERVER LOCAL
    aaa authentication ssh console AAA-SERVER LOCAL
    aaa authentication serial console AAA-SERVER LOCAL
    aaa authentication http console AAA-SERVER LOCAL
    aaa authorization exec authentication-server

http server enable
http 10.4.48.0 255.255.255.0 inside
snmp-server host inside 10.4.48.35 community *****
    no snmp-server location
    no snmp-server contact
    snmp-server community *****
    snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
    sysopt noproxyarp inside
    sla monitor 16
        type echo protocol ipIcmpEcho 172.18.1.1 interface outside-16
    sla monitor schedule 16 life forever start-time now
    crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
    crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
    crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev1 transform-set ESP-AES-128-SHA ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set reverse-route
crypto map outside-16_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
crypto map outside-16_map interface outside-16
crypto ca trustpoint CVD-ROOT-CA
  enrollment terminal
crl configure
crypto ca trustpoint CVD-Issuing-CA
  enrollment terminal
crl configure
crypto ca trustpoint VPN-ASA5525X-Cert
  enrollment terminal
  fqdn VPN-ASA5525X.cisco.local
  email admin@cisco.local
  subject-name CN=VPN-ASA5525X.cisco.local
  ip-address 172.16.130.122
  keypair VPN-ASA5525X-Keypair
  no validation-usage
crl configure
crypto ca trustpoint VPN-ASA5525X-FO-Cert
  enrollment terminal
  fqdn VPN-ASA5525X-FO.cisco.local
  email admin@cisco.local
  subject-name CN=VPN-ASA5525X-FO.cisco.local
  ip-address 172.17.130.122
  keypair VPN-ASA5525X-Keypair
  no validation-usage
crl configure
crypto ca trustpoint policy
crypto ca certificate chain CVD-ROOT-CA
certificate ca 4e880aa7904ed6b04e8a8b63e9b514b2b 30820343 3082022b a0030201 0202104e 880aa790 4ed6b044 ea8b63e9 b514b230 0d06092a 864886f7 0d010105 05003034 310c300a 06035504 0b130363 7664310e 300c0603 55040a13 05636973 636f3114 30120603 55040313 0b435644 2d524f4f 542d4341 301e170d 31343035 31353134 31313333 5a170d32 34303531 35313432 31333335a 3034310c 300a0603 55040b13 03637664 310e300c 06035504 0a130563 6973636f 31143012 06035504 03130b43 56442d52 4f4f542d 43413082 0122300d

Appendix C: Configuration Files August 2014 Series
Appendix C: Configuration Files

August 2014 Series

quit
crypto ca certificate chain CVD-Issuing-CA
certificate ca 77000000135662b8af34a01af0000000000013
30820422 3028030a a0032001 02021377 00000013 5662b8af 34a01af0 00000000
0013300d 06092a86 4886f70d 01010050 00303431 c0300a06 0355040b 13036376
64310e30 0c060355 040a1305 63697363 6f311430 12060355 0403130b 4356442d
524f4f54 2d434130 1e170d31 34303830 33303330 3730357a 170d3139 30383032
32032373 3037593a 13060a09 92268993 f2c64a01 1961056c 6f63616c
31153013 060a0992 268993f2 2c640119 16053639 73636f31 17301506 03550403
130e4356 442d4973 7375696e 672d3431 0820122 300d0609 2a864886 f70d1010
01050003 820010f0 02820101 0a7b7f2 18465440 6e7747ca 2a4b33a0
05f1def4 e308fff0 27c68f59 7b33b6e0 ced1f635 0558272a 19ed588c a78b8070
79ac0349 80c95b0d 29e3eeff fa05fb47 973b1def c683b967 b0636c9 fd285df9
71cd6160 59f18c08 778f4bfb 92705e01 3c7d2a8b 08ef8f02 0d8a4ad9 67749859
77dc49b1 9b649788 e7a3e089 09d6f074 e92ba9a8 3d1e6007 600f3bfc e63062b0
eac7e907 a1278741 a70a435 db98aee3 a2890e6d 5d931c4b 4bbbc14 58955f5c
38cd9d18 18b97ad5 924c1a46 e36eddbd b0e91100 11e2a5f4 67e8038d
cb5f3b52 b07f6dc5 b2f9dc72 f7d01586 10c0de74 b6ddf6c3 70d7c0d6 cb2218d
93da3447 2f1980be eaa5dd5b f55ce0a2 07020301 0001a382 01138082 01143010
06092b06 01040182 37150104 03020100 301d0603 551d0e04 1604174d 6241fca
8c0c5bc3 3f6c1ee7 1c0adcb7 c5fe7d30 43060355 1d20043c 303a3038 06082a03
048b2f43 5905302c 302a0608 2b060105 05070201 161e6874 74703a2f 2f706e69
2e636973 636f626c 6f63616c 2f637073 2e747874 30190609 2b060104 01823714
02040c1e 0a055300 75062002 400413b0 30060355 1d0f0404 03020186 300f0603
551d1301 01ff0405 30030101 ff301f0f 03551d23 01183016 0143d7e 650f3b6c
ed6ed9d fd5527ab f92ebb52 19283042 0603551d 1f043b30 393037a0 35a03386
Appendix C: Configuration Files

August 2014 Series

36

quit
certificate ca 770000001315662b8af34a01af000000000001
30820422 3082030a a030201 02013177 00000013 5662b8af 34a01af0 00000000
0013300d 0609a06a 486ff7d0 01010505 00303431 0c300a06 0355040b 13036376
64310e30 0c060355 040a1305 63697363 6f311430 12060355 0403130b 4356442d
524ff5d4 2d4d3410 1e170d31 34303830 38320301 3703075a 170d3139 30383038
32303237 30375a30 47311530 13060a09 92268993 f22c6401 1916056c 6f63616c
31153013 060a9929 68399f32 2c640119 16056369 73663f31 17301506 3550403c
130e4356 442d4973 737569e6 672d3410 30820122 300d0609 2a864886 f70d0101
01050003 82010f00 3082010a 02820101 0a7b7f02 18465440 6e7747ca 2a63503a
05f1def4 e308ff00 27c6ff59 7b33b6e0 cedf63f5 058527a2 19ed588c a78b8070
79ac0349 5c095b00 6739eef3 2b5e73e6 6b3845c3 3f6c1e77 1c0a0c35 0b88a6e3 a28906e6 5d93134c 4bb11c4 5895f5ac
38cd9d18 18b97ad5 924c146a e36edbd8 b0e91100 11e2a5f4 1b7c388 67e8038d
cbcf3b52 b7f6dc5 b2f9dce7 7f0d1586 10c0de74 6f6df2c3 70dcd7cd 6cb2218d
9d3a3447 2f1980be aea5dd5b f55ce0a2 07020301 0051382 01183082 01143010
06092b06 0140182 37150104 03002100 301d0603 51d0e04 1604147d 6241fca4
8c0c5bc3 3f6c1e77 1c0a0c35 0b88a6e3 a28906e6 5d93134c 4bb11c4 5895f5ac
48bf2f43 5905302c 302a0608 2b060105 05070201 161e6874 74703a2f 2f706b69
2e636973 63f6e26c 6f63616c 2f637073 2e747874 30190609 2b060104 01823714
02040c1e 0a005300 75006200 43060355 1d20043c 303a3038 06082a03
48bf2f43 5905302c 302a0608 2b060105 05070201 161e6874 74703a2f 2f706b69
2e636973 63f6e26c 6f63616c 2f637073 2e747874 30190609 2b060104 01823714
02040c1e 0a005300 75006200 43060355 1d20043c 303a3038 06082a03
551d1301 01ff0405 30300101 ff30010f 03551d23 04183016 8014c7e 650f3b6c
eb6ed99 fc5527ab f92e6b52 19823042 0603551f 1f043b30 39037a0 35a3386
31687474 70af2f7f 7063e6cf 63697363 6f62e6cf 636126cf 43657247 456e726f
6c62f43 56442d52 4f4f542d 43412e63 726c300d 06092a86 4886f70d 01010505
00038201 01003efd 1cc70f10 3f6f6935 73ebd6dc d92ffba0 8897eafe af0a0bb5
87173150 a5109e09 98f572d c9c5f557 f3e64ae9 d3406ded 7957ce14 1b553ca2
49baabaf dc24533a 17f88a33 73f6d5b 25738798 baf386c1 bf02b3aa 4a454995
0f15e71e e779d1a 00170f02 24e9399d cbf70908 59fb882b 3397325 83df324
9df52c2d 3df9607 6ca1f9ac 001c6100 84400e42 8666e49 c0a7d8ea 12fc4fc2
9b8065bd a382baa 72a95f6 1f66c2c1 02a05997 920ce639 1be5d102 175418d2
59a7bade 5c5f692 59eacddc fc3ced61 b3608df 770080e 4735c5fa a46281e3
be2e2e3 04a8825 3dc83751 4f69ed27 33406bc8 c526557 2f78108 911f3699
92bdffdb 5151

quit
crypto ca certificate chain VPN-ASA5525X-FO-Cert
Certificate 61e9962b0000000000014
30820544 3082042c a0030201 02020a61 e9962b00 00000000 14300d06 092a8648 86f70d01 01005000 30473115 3013060a 09226829 93f22c64 01191605 6c6f6361 6c311530 13072e31 3302e31 3232312a 30280609 2a864886 f70d0109 0213b56 5042e2d4 53413535 3235582d 464f2e63 6973636f 6c6f6361 301d001b 06020500 92a2a684 86f70d01 00080500 3082042c b08d82e0 61ea9572 01cb8b6b b96430a9 6302e6bb 7a1ba3a9 3da1167d 03ee400f 6b26ca5e 7b2405b9 e0423b1 e7b8553e d6c8abbb 1b783d2b 6a6fbf0d d62e053d 545bb478 f6593192 c8b60021 bbf439f6 b4bb0de1 518b627f e309fbab 4528b616 816db3eb b18ace20 e4010ff1 5911f3b6 93198c4e 3f6f5675 6dc5963d 8d8a9c37 f98ca5e4 5f32ac57 a065716c e06ad2a 70b95b33 2230c87a a6c403bd 61e5125c 0e6f4f62 95db86b1 edf9b2ae 9db2489 a577f32a 6eddf7ed 1d316c78 06ddef66 e6315abe 1e27951d 05f1431b 16a1eb73 d2363e4d bd8f9c9a 98b4b305 17445e35 0246a63e a1a51ab6 086ebf06 ad6c8ec5 b4620fc8 1cbfe88e 4eefebf04 c7a16b61 c175c8a5 2759c16a 4e0d8bd6 fc24597b quit certificate ca 77000000135662b8af34a01af0000000000013 30820422 3082030a a0030201 02021377 00000013 662b8af 34a1af0f 00000000
0013300d 06092a86 4886f70d 01010505 00303431 0c303430300a060505000430300a060505010500030201003efd1cc7f01f03f61693573ebd6dc d92ffba08897eaf0a0bb5a382baa372a95cf6766f6c2e2ac85997920ce6391be5d102175418d2e beb2cc014eaae8393dc837514f69ed2733406bc8c52c65572f87810691lf3699 92bdfdbd5151 quit crypto ikev1 enable outside-16 crypto ikev1 policy 10 authentication crack encryption aes-256 hash sha group 2 lifetime 86400 crypto ikev1 policy 20 authentication rsa-sig encryption aes-256 hash sha group 2 lifetime 86400
crypto ikev1 policy 30
authentication pre-share
encryption aes-256
hash sha
group 2
lifetime 86400
crypto ikev1 policy 40
authentication crack
encryption aes-192
hash sha
group 2
lifetime 86400
crypto ikev1 policy 50
authentication rsa-sig
encryption aes-192
hash sha
group 2
lifetime 86400
crypto ikev1 policy 60
authentication pre-share
encryption aes-192
hash sha
group 2
lifetime 86400
crypto ikev1 policy 70
authentication crack
encryption aes
hash sha
group 2
lifetime 86400
crypto ikev1 policy 80
authentication rsa-sig
encryption aes
hash sha
group 2
lifetime 86400
crypto ikev1 policy 90
authentication pre-share
encryption aes
hash sha
group 2
lifetime 86400
crypto ikev1 policy 100
authentication crack
encryption 3des
hash sha
group 2
lifetime 86400
crypto ikev1 policy 110
  authentication rsa-sig
  encryption 3des
  hash sha
  group 2
lifetime 86400
crypto ikev1 policy 120
  authentication pre-share
  encryption 3des
  hash sha
  group 2
lifetime 86400
crypto ikev1 policy 130
  authentication crack
  encryption des
  hash sha
  group 2
lifetime 86400
crypto ikev1 policy 140
  authentication rsa-sig
  encryption des
  hash sha
  group 2
lifetime 86400
crypto ikev1 policy 150
  authentication pre-share
  encryption des
  hash sha
  group 2
lifetime 86400
!
track 1 rtr 16 reachability
telnet timeout 5
ssh stricthostkeycheck
ssh 10.4.48.0 255.255.255.0 inside
ssh timeout 5
ssh version 2
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 10.4.48.17
ssl encryption aes256-shal aes128-shal 3des-shal
ssl trust-point VPN-ASA5525X-Cert outside-16
ssl trust-point VPN-ASA5525X-Cert outside-17
webvpn
enable outside-16
enable outside-17
anyconnect-essentials
anyconnect image disk0:/anyconnect-win-3.1.05160-k9.pkg 1
anyconnect image disk0:/anyconnect-macosx-i386-3.1.05160-k9.pkg 2
anyconnect profiles RA-Profile disk0:/ra-profile.xml
anyconnect enable
tunnel-group-list enable
group-policy GroupPolicy_Employee internal
group-policy GroupPolicy_Employee attributes
  banner value Group "vpn-employee" allows for unrestricted access with a tunnel all policy.
group-policy GroupPolicy_5505 internal
group-policy GroupPolicy_5505 attributes
  vpn-tunnel-protocol ikev1
  password-storage disable
  split-tunnel-policy tunnelall
  secure-unit-authentication enable
  nem enable
group-policy GroupPolicy_AnyConnect internal
group-policy GroupPolicy_AnyConnect attributes
  wins-server none
  dns-server value 10.4.48.10
  vpn-tunnel-protocol ssl-client
  default-domain value cisco.local
group-policy GroupPolicy_Partner internal
group-policy GroupPolicy_Partner attributes
  banner value Group "vpn-partner" allows for access control list (ACL) restricted access with a tunnel all policy.
  vpn-filter value RA_PartnerACL
group-policy GroupPolicy_Administrator internal
group-policy GroupPolicy_Administrator attributes
  banner value Group "vpn-administrator" allows for unrestricted access with a split tunnel policy.
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value RA_SplitTunnelACL
username admin password w2Y.6Op4j7c1Vdk2 encrypted privilege 15
tunnel-group AnyConnect type remote-access
tunnel-group AnyConnect general-attributes
  address-pool RA-pool
  authentication-server-group AD
default-group-policy GroupPolicy_AnyConnect password-management
tunnel-group AnyConnect webvpn-attributes
group-alias AnyConnect enable
group-url https://172.16.130.122/AnyConnect enable
group-url https://172.17.130.122/AnyConnect enable
tunnel-group Teleworker5505 type remote-access
tunnel-group Teleworker5505 general-attributes
  authentication-server-group AAA-SERVER
default-group-policy GroupPolicy_5505
  password-management
tunnel-group Teleworker5505 ipsec-attributes
  ikev1 pre-shared-key *****
  
class-map inspection_default
  match default-inspection-traffic
  
  
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512

policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect ip-options
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
    
  service-policy global_policy global
  prompt hostname context
  no call-home reporting anonymous
call-home
  profile CiscoTAC-1
  no active
    destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
    destination address email callhome@cisco.com
    destination transport-method http
    subscribe-to-alert-group diagnostic
    subscribe-to-alert-group environment
    subscribe-to-alert-group inventory periodic monthly 1
subscribe-to-alert-group configuration periodic monthly 1
subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:fc2f5629d41067885d8bf72400322745
: end

ASA-5505

ASA Version 9.1(5)
!
hostname TS01-ASA5505
domain-name cisco.local
enable password 2y4F1gBvYyBLau0Q encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
names
!
interface Ethernet0/0
  switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
  nameif inside
  security-level 100
  ip address 10.4.156.1 255.255.255.248
!
interface Vlan2
  nameif outside
  security-level 0
ip address dhcp setroute
!
ftp mode passive
dns server-group DefaultDNS
domain-name cisco.local
pager lines 24
mtu inside 1500
mtu outside 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
aaa-server AAA-SERVERS protocol tacacs+
aaa-server AAA-SERVERS (inside) host 10.4.48.15
  key *****
user-identity default-domain LOCAL
aaa authentication http console AAA-SERVERS LOCAL
aaa authentication ssh console AAA-SERVERS LOCAL
http server enable
http 10.0.0.0 255.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
crypto ikev1 policy 65535
  authentication pre-share
  encryption 3des
hash sha
  group 2
  lifetime 86400
telnet timeout 5
ssh stricthostkeycheck
ssh 10.0.0.0 255.0.0.0 inside
ssh timeout 5
ssh key-exchange group dh-group1-shal
console timeout 0
management-access inside
vpnclient server 172.16.130.122
vpnclient mode network-extension-mode
vpnclient vpngroup Teleworker5505 password *****
vpnclient enable
dhcpd option 150 ip 10.4.48.120
! dhcpd address 10.4.156.2-10.4.156.6 inside
dhcpd dns 10.4.48.10 interface inside
dhcpd domain cisco.local interface inside
dhcpd enable inside
!
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
username admin password w2Y.6O4j7c1vDk2 encrypted privilege 15
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect ip-options
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect smtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
  profile CiscoTAC-1
  no active
destination address http https://tools.cisco.com/its/service/oddce/services/ DDCEService
destination address email callhome@cisco.com
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodic monthly
subscribe-to-alert-group configuration periodic monthly
subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:614cfe033289e55a52925aa88c77cfa4
: end
Appendix D: Changes

This appendix summarizes the changes Cisco made to this guide since its last edition.

- We updated the Cisco ASA 5505 software to 9.1(5).
- We updated the RA VPN ASA configuration to explicitly disable proxy ARP for Identity NAT rules.
- We added detailed steps for creating an authorization profile and associated rules for VPN teleworker group on the Cisco ACS.
- We added topology diagrams.
- We created detailed steps for establishing the VPN tunnel.
Please use the feedback form to send comments and suggestions about this guide.