Cisco Collaborative Professional Services
Cisco Network Device Security Assessment Service

Secure network devices are foundational to the security of mission-critical networks and business data. Vulnerable devices potentially open the door to attacks that can compromise a network’s security defenses. The Cisco® Collaborative Professional Services Network Device Security Assessment Service helps partners maintain a hardened network device environment by identifying gaps in end customers’ network infrastructure security. The assessment data analysis is performed by consultants who draw upon their extensive security experience in industry and government agencies. This expertise is supported by a combination of Cisco best-in-class tools and methodologies and superior access to Cisco product development engineers to help you make the most of the sophisticated security features in your customers’ Cisco products.

Used during the build or manage phase of the network, as shown in Figure 1, the Cisco Network Device Security Assessment Service uses an internally developed configuration analysis engine to compare the customer’s device configurations with Cisco’s best practice recommendations. These results are then verified and augmented by experienced Cisco security consultants to create a customized list of recommendations.
Cisco network security consultants will examine the device configurations to identify:

- Opportunities to enhance device hardening by implementing security best practices to reduce attack surface and known vulnerabilities
- Opportunities to deploy device-level security configurations to improve the security architecture of the network
- Configuration inconsistencies across the deployed network and security devices

**Benefits**

The Cisco Network Device Security Assessment Service offers these benefits:

- Significantly reduces the risk of an adverse security event
- Enhances a partner’s business and operational agility by enabling the partner to launch a new Network Device Security Assessment Service anytime and anywhere, with minimum investment
- Offers access to innovative Cisco security configuration analysis tools and an industry-proven security infrastructure methodology implemented by Cisco security consultants with extensive industry deployment experience and knowledge of best practices
- Enables a partner to harden a customer’s Cisco network devices by identifying gaps in the security configurations of the devices, thereby improving the security of the overall architecture
Cisco Network Device Security Assessment Service Deliverables

The Cisco Network Device Security Assessment Service includes the deliverables described in Tables 1 and 2.

**Table 1. Cisco Network Device Security Assessment Service**

<table>
<thead>
<tr>
<th>Service</th>
<th>SKU</th>
<th>What It Does</th>
<th>Report Details</th>
<th>Specializations Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Network Device Security Assessment Service</td>
<td>ASF-CPSA-NDSA</td>
<td>Performs an automated analysis of supported network devices connected to the network, including core routing and switching and firewalls, and helps partners implement and maintain a hardened network device environment by identifying gaps in the security of the customer’s Cisco network infrastructure</td>
<td>Network Device Security Assessment Report • Executive Summary • Register of Recommendations • Detailed Analysis Results</td>
<td>Aligns with eligibility for product resale</td>
</tr>
</tbody>
</table>

**Table 2. Cisco Network Device Security Assessment Service Report Details**

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>• Provides a high-level, executive view of the key findings from the assessment, identifying potential security risks and key recommendations</td>
</tr>
<tr>
<td>Register of Recommendations</td>
<td>• Summarizes the identified security issues and recommendations to mitigate the risks to enhance the security posture of the customer’s network devices</td>
</tr>
<tr>
<td>Detailed Analysis Results</td>
<td>• Provides a detailed analysis of the customer’s Cisco devices compared to Cisco and industry best practices, identifying recommendations to mitigate the identified risks</td>
</tr>
</tbody>
</table>

**Collector Specifications**

The Network Device Security Assessment Service uses the Cisco Common Services Platform Collector (CSPC), a modular, flexible, reusable collector platform that collects data from customer network devices and servers. Partners will be provided with instructions for downloading and installing the software, as well as for uploading the collected data for analysis by Cisco network engineers.

Cisco recommends the following system and hardware specifications:

- Desktop or any hardware running an Intel Pentium processor or later and Microsoft Windows XP/2000/ME
- 4 GB RAM or more is recommended
- Network connectivity such as Ethernet or wireless to connect to the server

Devices included in the collection must be accessible through Simple Network Management Protocol (SNMP) and telnet polling. Collected data is encrypted and transmitted to Cisco using the CSPC.

**Sizing and Limitations**

The Network Device Security Assessment Service covers a maximum of 250 devices among the following Cisco products:

- Cisco routers running the Cisco IOS® and IOS XE operating systems
- Cisco Catalyst® switches running the CatOS operating system
- Cisco ASA firewalls and firewall services modules
- Cisco PIX® firewalls
Engagement

The Cisco Network Device Security Assessment Service is delivered remotely from Cisco’s Centers of Excellence. Project kickoff and delivery begins within seven business days of order placement. Table 3 describes the roles and responsibilities of Cisco and the partner in delivering the Cisco Network Device Security Assessment Service.

Table 3. Roles and Responsibilities

<table>
<thead>
<tr>
<th>Phase</th>
<th>Owner</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1. | Cisco | ● Cisco Project Manager schedules and conducts the project kickoff with the partner.  
● Cisco Project Manager creates and publishes the project schedule. |
| 2. | Partner and customer | ● Partner works with the customer to familiarize them with the service, set expectations, and collect information about the customer’s network. |
| 3. | Partner | ● Partner downloads, installs, and configures the collector software. |
| 4. | Partner | ● Partner runs the collector software on the customer’s network for a 24-hour period.  
● Partner uploads the collector data to Cisco. |
| 5. | Cisco | ● Cisco network engineers analyze the uploaded data using Cisco intellectual capital.  
● Cisco produces the reports with recommendations. |
| 6. | Partner | ● Partner reviews the reports, adds its own recommendations, and creates final reports for the customer. |
| 7. | Partner and customer | ● Partner and customer review the final reports together, agreeing on recommendations to implement. |
| 8. | Partner | ● Partner implements the recommendations on the customer’s network. |