Cisco 7200 Series and 7301 Routers
Security Services
AGENDA

- Cisco® 7200 Series and 7301 Routers Profile and Security Positioning
- Cisco 7200 Series and 7301 Routers Security Services
  - Threat Defense and Embedded-Services Management
  - Secured VPN Services
  - Secured Connectivity, Trust, and Identity
  - Secured Cisco IOS® Software
  - Security Certifications and Evaluations
Current Security Challenges

• Challenges in deploying and managing multiple devices
  Multiple devices to troubleshoot
  Multiple operating systems to learn

• Worms and viruses increasing monthly
  Limited IT staff at small and branch offices available to combat these challenges
  DDoS & DoS targeting hosts and network devices
  Increased attacks at all points of the network

• Legal obligations require more due diligence
  Health Insurance Portability & Accountability Act (HIPAA)
  Gramm-Leach-Bliley Act (GLBA)
  EU Data Protection Act
Security at Cisco

Cisco's number one priority and focus is on the success of our customers. We are committed to helping customers with securing their network environment through best practice sharing, innovative and resilient network products, technologies, and services.

http://www.cisco.com/security/

"I truly believe that Cisco is uniquely positioned to deliver robust, scalable, and innovative security solutions. Because we at Cisco view security as an integrated process, we understand the requirements necessary to implement a secure, robust networking environment. Our goal is to minimize risk while maximizing productivity opportunities through integrated network security solutions."

– John Chambers
Cisco Self-Defending Network Strategy

Cisco® strategy to dramatically improve the network’s ability to identify, prevent, and adapt to threats

INTEGRATED SECURITY
- Secure Connectivity
- Threat defense
- Trust & identity

SECURITY TECHNOLOGY INNOVATION
- Endpoint security
- Application firewall
- Network anomaly detection

SYSTEM-LEVEL SOLUTIONS
- Endpoints, networks, and policies
- Services
- Partnerships
Cisco 7200/7301 Routers
Profile and Security Positioning
Cisco IOS Software is the Common Denominator

Cisco® Secured Router

Cisco IOS® Security
- IPSec
- PKI
- Firewall
- Intrusion prevention
- SSH
- SSL
- 802.1x
- AAA
- ACLs
- NAT
- Infrastructure features

Cisco IOS IP Fabric

Internet Application Technologies
- Security
- VoIP
- Video
- Multicast
- VPN
- SNA Evolution
- Load Balancing
- Caching
- Address Mgmt
- ...

Operational Security
- SSHv2
- SNMPv3
- 16 Privilege levels
- MD5 encrypt pswds
- AAA Authentication
- AAA Authorization
- Infrastructure Sec
- Auto Secure

Cisco.com
Cisco IOS Security Routers
Advanced Network and Security Integration

- Unparalleled modularity and deployment flexibility
- Advanced site-to-site VPN solution
- Stateful firewall and in-line intrusion prevention
- VoIP gateway and content services
- Integrated security device manager
- Robust remote management

www.cisco.com/go/routersecurity
Cisco 7200 and 7301 Routers

Integrated Security Services

- Comprehensive integrated networking
  - Routing, WAN, LAN switching voice, content networking
- Integrated security services
  - Trust and identity with Network Admission Control, 802.1x and advanced AAA services
  - Secured connectivity for site-to-site and remote VPNs
  - Threat defense with intrusion prevention, Netflow, and firewall
  - Network infrastructure protection with Control Plane Policing, NBAR, and AutoSecure
- VPN application transparency
  - VPN support for multicast, latency-sensitive traffic, routing updates, and non-IP protocols
- V3PN
  - Delivers data, voice, and video with QoS for latency sensitive traffic
- VPN integration with Dynamic Routing Protocols
  - for scalable & resilient connectivity
- Reduced cost of ownership
  - Integrated functionality combined with single device / solution management lower TCO
Cisco 7200 and 7301 Routers Positioning

Enterprise Head End and SP Edge

- Cisco® 7200 Series routers are ideal for up to OC3 performance with integrated services
- Target enterprise core and service provider edge
- Diverse deployment applications:
  - WAN aggregation, Managed Security, IBM datacenter, SAA management, broadband aggregation, MPLS PE, and route reflector
- Modular engine options for improved performance
- High-density Port adopter supported across 7x00 platforms with onboard GE ports
- Supports hot-swappable modules and redundant power supplies
- Supported in both Cisco IOS® T, S, and Mainline releases where new enterprise features or stability are key requirements
Cisco 7200 and 7301 Switches Positioning
Head End and WAN Aggregation

Managed FR / ATM (higher BW)
Going to → Managed L2VPN / L3VPN

WAN Security Services
- Cisco IOS® Firewall
- Cisco IOS IPS
- App Firewall
- Trend Anti Virus
- IPSec VPN
- DMVPN Hub
- NAC
- Autosecure
- CPP
- EasyVPN server
- IP source tracker
- IKE DDoS prevention
- Role-based CLI
- AAA
- NetFlow Monitoring
- NBAR
Cisco 7200 and 7301 Switches Positioning

Broadband Aggregation

Broadband Security Services

- Per-user firewall
- Cisco IOS® IPS
- IPSec VPN
- Autosecure
- Trend antivirus
- DMVPN hub
- NetFlow monitoring

- EasyVPN server
- IP source tracker
- IKE DDoS prevention
- Role-based CLI
- AAA policy provisioning

DSL Router

DSLAM

ATM

PPPoX

DSL Modem and
PPPoE Client

LAC

PPPoX

L2TP

Cisco 7301 LNS + Cisco IOS FW

RADIUS

Syslog

Internet
Cisco 7200/7301 Switch Positioning

Provider Edge

Provider-Edge Security Services

- VRF aware IPSec
- VRF aware AAA
- VRF-aware Cisco IOS® Firewall
- NetFlow Monitoring

Internet or Partner Provider Network

MPLS, IP or L2 (ATM, FR) Network

IPSec VPN

MPLS VPN

Internet Access with per VRF Firewalls

VPN A

Customer A

VPN B

Customer B

VPN C

Customer C

Branch Office

Mobile Worker

Cisco Client

Local, Direct Dial ISP

Cable/DSL/ISDN ISP

Corporate Headquarters

Remote Site Internet Access with Per User Firewalls
Cisco 7200 and 7301 Router Security Services

Threat Defense and Embedded Services Management
Embedded Services Management
Cisco Router and Security Device Manager (SDM) 2.1

Integrated Management of Router Services
Routing, Switching, Security and QoS

Use the Cisco® TAC knowledgebase
to troubleshoot VPN and WAN

- Security Features
  - VAM2+ support
  - Firewall policy rules, syslog and logs
  - Inline IPS with Dynamic Signature update and signature customization
  - Role-Based Router Access
  - Easy VPN Server and AAA
  - Digital Certificates for IPSec VPNs
  - Security Audit
  - DMVPN Hub

- IP Services Support
  - OSPF, EIGRP, RIPv2, static
  - ACL and NAT policy definition
  - DHCP Pools

- New Wizards for non-experts
  - QoS Policy and NBAR

- New Troubleshooting tools
  - VPN, WAN connection

- Real-Time and Graphical router and network resource monitoring

http://www.cisco.com/go/sdm
Threat Defense
Cisco 7200 and 7301 Router Firewall Services

• Now offering an integrated IPsec/Firewall/IPS bundle
• Cisco IOS® Firewall
  – Stateful packet inspection – protocol anomaly detection
  – Support for advanced IPv4 protocol inspection (TCP, UDP, ICMP, H.323v2, SIP, Skinny, etc.)
  – IPv6 stateful inspection of TCP/UDP/ICMP/FTP traffic
  – URL filtering (Websense & N2H2)
  – Per-user firewalls
  – Transparent Layer 2 firewall
  – Per-user authentication/authorization for http/https, ftp, and telnet
  – Application Firewall (TCP Port 80 Policy Enforcement)
  – Per VRF Firewall
  – Denial of Service (DoS) detection and prevention
  – SMTP and ES-MTP attack mitigation and inspection
• Extensive NAT, ACL IP services included
Threat Defense
Cisco 7200 and 7301 Intrusion Prevention (IPS)

• Utilize Cisco® 7200 Series and 7301 routers to mitigate network violations and intrusions
  – Inline deep packet inspection enhancing network attack mitigation
  – Deployed to mitigate and remove known and current network threats

• Support of Cisco IDS 42xx Sensor signature files
  – Signatures can be downloaded and enabled without a restart of the entire router
  – Allows signature tuning and customization

• Provisioning and management
  – Cisco SDMv2.1 supports dynamic signature updates and tuning
  – IDS Management Center (MC) 2.3 manages/provisions both Cisco IOS IPS and IDS 42xx Sensors
  – Sensor/Router management protocol – SDEE supported
Threat Defense
Cisco 7200 and 7301 Intrusion Prevention (IPS)

- Prevent intrusion of known network attacks
  - 900 network attack and host exploit or virus vulnerabilities
    - **Sample worms/virus**: Phatbot, Agobot, GaoBot, Nachi, Blaster, NIMDA, Scalper, Apache, Slapper, Gnutella, Klez, Ants, Mimail Virus, Novarg/Mydoom
    - **Sample attacks**: PingOfDeath, TCPFRAGSYN/FINPacket, DNSSQUERYOverflow, Back Orifice Ping, Trinoo, Deep Throat Response, Morpheus
  - Embedded with SDM 2.1 file package or download from CCO
  - Provisioning by IDS MC (same as IDS sensor provisioning)
Threat Defense
Cisco 7200 and 7301 Anti Virus Support

- Prevent intrusion of known viruses using Trend Micro intelligence
- Downloaded by way of Cisco.com (CCO IDS Signature database)
- Subscription services – 0 day virus anywhere in the world
  - Pushed to the Cisco® router
  - Within 15 minutes receive a crude policy, immediate mitigation
  - Within 2 hours receive a fine grain policy, more discrete

Customer

- Cisco IPS 4200 Series
- Cisco Catalyst® 6500 IPS Blade
- ASA 5500 SSM Blade
- “Mohawk” Router Blade
- Cisco IOS® IPS c83x-c7xxx

Cisco

- VMS
- Regular IPS Signatures
- Policy (coarse filter)
- Signature (fine filter)
- Cisco Incident Control Center (CICC)

Cisco

- IPS Engineering Signature Integration
- IPS Signature Update Server
- Policy (coarse filter)
- Signature (fine filter)

Trend Micro

- TrendLabs Servers
- Regular AV Signatures
- Malware Outbreak!
- Cisco Trend Micro Policy (coarse filter)
- Signature (fine filter)

Cisco Incident Control Center (CICC)
Convergence of Firewall and Inline IPS technologies have given birth to the next-generation firewall: Application Policy and Control

Advanced HTTP deep-packet inspection services help protect from Web-based attacks and other types of “port 80 misuse”

Enables policy definition and enforcement for tunneled traffic
  – Instant Messaging (AIM, MSN Messenger, Yahoo)
  – Peer-to-peer (KaZaA)

Provides HTTP RFC compliance to detect protocol anomalies
Provides MIME type filtering and content validation
Threat Defense
NetFlow—Monitoring for Anomaly Detection

• High-level diagnostics to classify and identify network anomalies

• NetFlow records can help classify an attack
  – Generates and provides detailed flow information
  – What is being attacked and who/where the attack originated
  – How long the attack is taking place
  – Size of packets used in the attack

• NetFlow records sent to external Cisco® Router Security partners
  – Application hosts correlate and analyze information
  – Arbor Networks, Protego, Mazu, and Adlex
  – Analyzing NetFlow records identify changes in network behaviour which are declared network anomalies
  – Partner application raises alarms based on predefined rules to minimize inundating operations with low risk incidents (alarms)

• Enables router to mitigate further attacks by allowing operations to load appropriate ACLs, firewall rules, attack/virus signatures, etc.
Threat Defense
Correlation and Mitigation Tools

- Anomaly Detection
- Aggregation & Preprocessing
- Correlation
- Provisioning
- Alarms, Netflow, etc

Push policy or enable signatures

- Architect the network with IDS Sensors
- Aggregate network information
- Correlate
  - Cisco® Protego or
  - Arbor Networks or
  - NetForensics
- Push policy to routers
  - Firewall rules
  - IPS Attack, Exploit or Virus Signatures
  - ACLs
  - Route tables
  - QoS
  - Etc…
Threat Defense
Network-Based Application Recognition—NBAR

- Independent of firewall and IPS services
- Intelligent Classification Engine used in conjunction with QoS class-based features
- Protocol Discovery analyzes application traffic patterns in real time and discovers which traffic is running on the network
- IP packet classifier capable of classifying applications that have...
  - Statically assigned TCP and UDP port numbers
  - Non-TCP and Non-UDP IP protocols
  - Dynamically assigned TCP and UDP port numbers during connection establishment
  - Sub-port classification able to look deeper into packet to identify applications
- Currently supports 85 protocols/applications
- Customization capability identifies Day 1 attacks/virus’
  - NBAR was used to mitigate Nimda, MyDoom and others in the Cisco® network
  - Used for static TCP/UDP port based applications that are not supported in NBAR
  - Up to 10 custom applications can be added
  - Map 16 TCP and UDP ports each per application
  - Statistics appear in the Protocol Discovery
Cisco 7200 and 7301 Router Security Services

Secured VPN Services
Secured VPN Services

IPSec VPN Solutions Positioning

**Dynamic Multipoint IPSec VPNs**
- Simplified scaling and mgmt.
- Traffic-based dynamic tunnels

**Routed GRE/IPSec**
- The power of Cisco IOS® networking applied to VPNs
- Full routing, application support, instrumentation

**Easy VPN**
- Ease of deployment

**Standard IPSec**
- Full standards compliance
- Interoperates with other vendors
  
  *Example: Extranet VPN*

**Dynamic Multipoint VPN:**
- On-demand VPNs

**Routed GRE/IPSec:**
- Proven Cisco IOS networking

**Easy VPN IPSec**
- Policy push for easy deployment
- High scalability at low cost

**Improved Productivity**
Secured VPN Services
Network Based IPSec VPN Services

Internet/Partner Provider Networks
Cisco IOS® Router
Branch Office
Cisco® Client 3.x/4.x
Mobile Worker
Telecommuters
Cisco Client 3.x/4.x
Or Cisco IOS Router

VPN Service Expansion

Existing VPN Infrastructure

Service Provider MPLS Network
IP Solution Center (ISC 3.0) (IPSec and MPLS Provisioning)
PE
VPN A
Customer A
VPN B
Customer B
Corporate Headquarters

1 Box or 2 Box Solution
PE
Branch Office A
Branch Office B

IP, MPLS or Layer 2 VPN

IPSec Session

BEMR BU Security © 2004 Cisco Systems, Inc. All rights reserved.
Secured VPN Services
Cisco 7200 IPSec Stateful Failover

• Ensures IPSec sessions continue in the event of a failure of the primary router

• 12.3(11)T features include:
  – Supports up to 2000 tunnels
  – Hot Standby Router Protocol (HSRP) for IP redundancy and interface tracking
  – SSO for transporting and maintaining state information between the active and standby routers
  – Hardware support for 7200VXR with NPE-G1, NPE-400, NPE-225 and VAM and VAM2

• 12.3(11)T1
  – Adds support for 7301

• 12.3(14)T
  – Adds support for VAM2+ and PKI
Secured VPN Services

VPN Acceleration Module (VAM) and VAM2

VAM

Functionality:
- Supported on Cisco® 7200, 7401 routers
- Provides up to 145 Mbps 3DES
- Supports Up to 5000 Tunnels

Cisco IOS® Train Support:
- 12.2T, 12.1E, 12.3, 12.3T

Orderability:
- Part #: SA-VAM
- Included with 7200/VPN bundles

VAM2

Functionality:
- Supported on Cisco 7200, 7301 routers
- Provides up to 260 Mbps 3DES
- Supports Up to 5000 tunnels
- Adds AES-128 bit keys in HW

Cisco IOS Train Support:
- 12.3, 12.3T

Orderability:
- Part #: SA-VAM2
- Included with 7200/VPN bundles
Secured VPN Services
Cisco 7200/7301 Security Bundles with VAM2

Bundle Components

- **7206VXR400/2VPNK9**: Cisco 7206VXR chassis with NPE-400, I/O with 2 F/E ports, VAM2, 256-MB system memory, AC power, IOS IP IPSec software

- **7206VXR225/2VPNK9**: Cisco 7206VXR chassis with NPE-225, I/O with 2 F/E ports, VAM2, 128-MB system memory, AC power, IOS IP IPSec software

- **CISCO7301/2VPNK9**: Cisco 7301 chassis with NPE-G1, 3 GE/FE ports, VAM2, 256-MB system memory, AC power, Cisco IOS IP IPSec software

Security bundles with VAM2 offer:

- Higher encryption performance - up to 260 Mbps on 7200 and 370 Mbps on 7301
- AES hardware acceleration
- Easy migration for now EOL 7100 Series and EOL 7400 VPN bundle
Secured VPN Services
VPN Acceleration Module 2+ (VAM2+)

Functionality:
• Adds hardware acceleration for AES wide keys (192 - 256-bit)
• Provides >260 Mbps 3DES (small performance boost over VAM2 with mid to large-size packets)
• Supports up to 5000 IPSec tunnels
• Hardware accelerated IPPCP compression

Platform Support:
• 7200 with NPE-G1, NPE-400 or NPE-225 processors
• 7301

Cisco IOS® Train Support:
• Targeting 12.3(12) and 12.3(11)T3 releases

Orderability:
• Part #: SA-VAM2+
• Included with new 7200 and 7301 security bundles
Secured VPN Services
Cisco 7200/7301 VAM2+ Security Bundles

• New VAM2+ security bundles
  – Cisco® 7206VXRG1/2+VPNK9
  – Cisco 7206VXR400/2+VPNK9
  – Cisco 7301/2+VPNK9

• Consistent with current bundle pricing but…
  Added benefits:
  – Adds hardware acceleration for AES wide keys
  – Includes additional system memory – 512 MB
  – Upgraded Cisco IOS® Software to include IP FW/IDS IPSec rather than IP IPSec

• Available Now

www.cisco.com/go/securitybundles
Cisco 7200 and 7301 Router Security Services

Trust & Identity and Secure Connectivity
Trust & Identity

Key Features

• Secure Shell (SSH)
  – SSHv2
  – Secure Copy (SCP)
  – SSHv2 Client

• SSL VPN in Cisco IOS® Software
  – Phased development
  – HTTP/HTTPS application support
  – TCP Port Forwarding for E-mail (SMTP, IMAP, POP3)
  – Radius/AAA-based Authentication
  – GUI-based Device Management

• 802.1x
  – 802.1x Authenticator

• PKI
  – Cisco IOS Certificate Server

• Network Admission Control (NAC)
NAC Solution: Leverages the network to intelligently enforce access privileges based on endpoint security posture.

Coalition of market-leading vendors:

- Focused on limiting damage from viruses and worms
- Limits network access to compliant, trusted endpoints
- Restricts network access by noncompliant devices
- Supports multiple AV vendors & Cisco Security Agent
- The 7200 and 7301 Security Bundles ship with NAC capability
Secure Connectivity

V3PN: Secure, Toll Quality Voice, Video, Data

V3PN:
- IPSec VPN tunnel built over GRE interface for site to site access
- Data, voice, and video traffic delivered with QoS policies for latency sensitive traffic

Benefits:
- Wirespeed encryption
- Bandwidth conservation
- Toll quality, jitter-free voice and video
- LAN and WAN security
Secure Connectivity
**Dynamic Multipoint VPN (DMVPN)**

**How DMVPN works**
- Spoke A needs to contact Spoke B
  - V3PN Call
  - PC Contact to a Server
- Learns real address of Spoke B via NHRP, OSPF or EIGRP (routing features)
- IPSec VPN tunnel to Spoke B is dynamically built over mGRE interface

**Benefits**
- Full Meshed connectivity with configuration simplicity of hub and spoke
- Preserves (central) bandwidth, minimizes latency
- Support for dynamically addressed spokes
- Zero touch configuration for addition of new spokes in the DMVPN

---

**Automatic Secure Meshed Tunnels**

[Diagram showing Hub, Spoke A, and Spoke B with different types of tunnels and IP addresses]
Secure Connectivity

*Easy VPN*

- Head end can be a Cisco 7200 or 7301 Router
- Remote/branch device can be a Cisco IOS Router, Cisco PIX® Firewall, VPN3002, or Cisco client software on a PC/Mac/Unix computer
- Remote device contacts central-site router/concentrator, and provides authentication credentials
- If credentials are valid, central-site “pushes” configuration data securely to the remote device and VPN is established
Secure Connectivity
Multi-VRF and MPLS support

• Cisco® 7200 and 7301 Router support for Multi-VRF (Virtual Routing and Forwarding) technology provides:
  – Multiple VRF per Customer Edge router
  – VRF IPSec mapping
  – VRF Firewall mapping

Support multiple organizations with overlapping IP addresses while maintaining separation of data, routing, and physical interfaces
Cisco 7200 and 7301 Router Security Services

Secured Cisco IOS Software
Secured Cisco IOS Software

Network Infrastructure Protection

- **AutoSecure**
  - Provides vital security recommendation with a straightforward "one-touch" device lockdown process/

- **Control Plane Policing**
  - Protects access to control plane, even during DDoS attacks. Monitors packets, increases infrastructure reliability, and availability/

- **Role-based CLI Access**
  - Provides partitioned, non-hierarchical, access to CLI commands for secure, logical separation of router users (eg. NetOps and SecOps)/

- **Netflow monitoring**
  - Provides early warning while visibility on traffic flows help you optimize network availability/

- **Out-of-band management**
  - Ensures access despite DoS attacks, or congestion/

- **Network-based Application Recognition (NBAR)**
  - Helps identify worms and other attacks by tracking Layer 4-7 applications and protocols/
Secured Cisco IOS Software
Cisco 7200 and 7301 Router AutoSecure

- **Disable Nonessential Services**
  - Eliminate DoS attacks based on fake requests to router services
  - Disable mechanisms that could be used to exploit security holes

- **Enforce Secure Access**
  - Enforce enhanced security in accessing device
  - Enhanced security logs
  - Prevent attackers from knowing packets have been dropped

- **Secure Forwarding Plane**
  - Protect against SYN attacks
  - Anti-Spoofing
  - Enforce stateful firewall configuration on external interfaces for firewall images

cisco.com/go/autosecure
Packets destined to the control plane consume valuable RP resources
- Router can be attacked by sending large amount of traffic (like ICMP) to be punted to the RP (the Control Plane)

Policing incoming traffic to the control plane (RP), reduces the incoming traffic rate, thus alleviating the DoS attack
Secured Cisco IOS Software
Role-Based CLI Access or Split Management

Security Engineer
- Firewall, IDS, IPSec, AAA...
- show

WAN Engineer
- Config
- Show
- Etc

Customized Access
To Match
Operational Needs

- Provide a View-based Access to CLI Commands
- A “view” is defined as a set of operational commands and configuration capabilities.
- User authentication is done via an external AAA Server (or TACACS+)
- Customer can define up to 15 views (in addition to 1 reserve for root user)

Example of defining a CLI View:
parser view first
password 5 <password>
command include exec show version
!
Command also available to list all views:
show parser view all
Cisco 7200 and 7301 Router Security

Certifications and Evaluations
Certifications and Evaluations
Cisco IOS Firewall

- ICSA Firewall 4.1, Corporate Category
  - Current: 12.3(11)T – Cisco® 1841 through Cisco 3845
  - In Progress: Cisco 7200 and Cisco 7301
  - Target Complete June 2005

- Common Criteria - Firewall
  - In Progress: EAL4+ US Protection Profile (PP) medium robust conformance
  - Target EAL4 NIST validated by Dec '05
  - Cisco 7200 and Cisco 7301 routers
www.cisco.com/go/securitycert
Certifications and Evaluations
Cisco IOS IPsec

- Cisco® Router Technology Group participates in 3 major industry Certifications for IPsec.
- (Specific model certified under each certification can be found at [http://www.cisco.com/go/securitycert](http://www.cisco.com/go/securitycert))
- **FIPS 140–2** “This standard specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information” (US, Canada, UK)
  - FIPS 140-2 level 2, FIPS-192 AES (Specific for AES)
  - Stringent review of product is done by the NIST (both HW & SW [http://csrc.nist.gov/cryptval/](http://csrc.nist.gov/cryptval/))
- **Common Criteria** – Evaluation process for Information Assurance (IA) “This multipart standard, the Common Criteria (CC), is meant to be used as the basis for evaluation of security properties of IT products and systems”
  - Mutually recognized by 15 member countries
  - NIAP = Joint NSA/NIST program serves as the US Common Criteria “NIAP Certification” = Common Criteria
- **ICSA** – Commercial security certification with testing programs in Firewall, IPSec Interoperability, etc.
  - [http://www.icsalabs.com/](http://www.icsalabs.com/)
## Certifications and Evaluations

**Cisco 7200 Series Router Certified Security Releases**

<table>
<thead>
<tr>
<th>Certification</th>
<th>Completed</th>
<th>In Progress</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICSA - IPSec</td>
<td>7204 12.2(11)T (attested only)</td>
<td>7206 VAM2</td>
</tr>
<tr>
<td>ICSA 4.1 - FW</td>
<td>Target Complete Jan 05</td>
<td>7206VXR, 7301</td>
</tr>
<tr>
<td>FIPS-140</td>
<td>7206 ISA 12.1(9)E, 7206 VAM 12.3(3d), 7206 VAM2 12.3(3d)</td>
<td></td>
</tr>
<tr>
<td>CC/EAL4 - IPSec</td>
<td>7204, 7206 ISA 12.2(6), VAM 12.1(10)E</td>
<td>7204, 7206 VAM2 12.3(5); 7301</td>
</tr>
<tr>
<td>CC/EAL4+ - FW</td>
<td>Target Complete Dec 05</td>
<td>7206VXR, 7301</td>
</tr>
</tbody>
</table>

For more security certification details: [http://securitycert.cisco.com/page/home](http://securitycert.cisco.com/page/home)