12VPN1 – VPN Part 1

Hello and welcome to part one of the “Cisco on Cisco” seminar on hardware VPN best practices. I'm Mike Swartz, a Project Manager in the Cisco IT Network Access Team. With me is David Iacobacci, a Network Engineer in the Cisco IT Network Access Team. Together, we have about 10 years of experience in Cisco IT building network access services for Cisco employees. The theme of our show today is hardware VPN at Cisco, an overview of how IT is designed, and deployed. A home access service for our employees that provides them with a secure, high performance enterprise class teleworker solution. In part one, we will provide an overview of the Cisco IT hardware-based VPN solution running IOS routers in our employee's homes. We will show you how we design a service; provide some details about the security features of this service. As well as how DMVPN technology adds to the service capabilities. And in part two, we will show you how we deploy and manage the service. We will also hold a short question and answer session and finish with a slide with further resources for you. So sit back and enjoy as we explore Cisco IT's use of hardware-based VPN to support home offices for Cisco employees.

HARDWARE VPN AGENDA

On the agenda of today, we talk about access, market demands and the landscape. We talk about ECT how it is a business enabler to meet customer requirements, how ECT reduces TCO. How ECT is a solution, is site-to-site Cisco IOS-based VPN, ECT as an end-to-end scalable VPN solution. And the ECT E2E VPN model with four pillars of security, connectivity, deployment and management, and finally best practices.

ACCESS MARKET DEMANDS AND LANDSCAPE

So let's talk about the access market. Today, customers require a VPN solution that provides secure end-to-end support for data, voice, video and wireless. Its simple, scalable, manageable, it allows the customers to easily subscribe or unsubscribe to modular services. And it has to be proven in real world scenarios, and it should be provided with best practices, lessons learned, how to deploy it and how to minimize TCO. The landscape. VPN's proven to become a big cost saver for enterprises. Industry is transforming from permanent circuits to the Internet as a super media. Residential broadband speeds are increasing and access numbers are growing, and the telecommuting lifestyle continues to grow, up to 60 million people by 2005. Clients continue to operate in a hostel environment as 70% of attacks are coming across the Internet.

ECT THE BUSINESS ENABLER MEETS CUSTOMER REQUIREMENTS

ECT meets customer requirements, it's manageable, and it minimizes TCO due to concepts like ZTD. That automates management and results in improved control of the remote devices. Its scalable, it can address the requirements of ISPs as well as large and small enterprises. Its secure, it supports layer of Cisco security features consistent with a self-defending network strategy. And transforms from integrated to collaborative, and later, adaptive security. It's a market distinguisher, it streamlines router configurations and integrates Cisco security with Cisco dynamic routing framework to create a solution only Cisco can offer. And it's flexible and modular, it responds and conforms and expands from secure data to IPT, Wi-Fi and video.

ECT REDUCES TCO

ECT produces TCO. Total cost of ownership generally consists of three parts, operational costs, acquisition costs and management costs. Reducing these components lowers TCO.

ECT SOLUTION CISCO IOS-BASED SITE-TO-SITE VPN

Cisco ECT solution is IOS-based site-to-site VPN, it does operate in either enterprise or ISP models. It uses a spoke router in the home network that has three VPN tunnels, two data and one management. The traffic is routed over the data tunnel in a failover model, and the management subnet is separate from the data subnet and can be physically isolated. So you could see in the picture that, in the home environment, we have a picture of Cisco phone, we have Wi-Fi and a computer connecting through the Internet. And then routing VPN tunnels back to Cisco's network over two data tunnels and one management tunnel.

ECT 3 PHASE APPROACH

ECT in Cisco IT is a three-phased approach, where phase one we have a hardware VPN architecture for home users using an 831 and replacing a 3002 VPN hardware VPN. It uses automated provisioning, it has secure and standardized management, and it uses of auth proxy for user authentication. Phase 2 benefits include automated provisioning of IP telephony; add security features like NBAR, IPS and 802.1x. Increases the office productivity levels close to the office and introduces multiple device types. Phase 3 benefits adds the 871 ISR router as the new standard CPE, it integrates secure management with wireless LAN. And it offers improved performance and throughput, which is something that customers will demand as Internet speeds increase.

ECT'S GLOBAL REACH IS SCALABLE

ECT in Cisco is global and it's scalable. You're looking at a map that shows where we have hubs today that are closest to our employees. To provide high availability as well as offering services such as voice, later video, and wireless.

ECT MANAGEMENT HUB

Now I'm going to turn it over to David, and he's going to talk a little bit more about ECT's architecture.

AUDIENCE COMMENT: Thank you, Mike. Here you have a snapshot of our typical ECT management hub; it is normally located in our data center. If you start at the upper right hand side, we have the ISC IP solution center. It is Cisco software running on Unix-based server; it is the brains, if you will, of our ECT solution. To the left of that, you have the IE2100, it's a Linux-based appliance and it is the CNS engine, it is the muscle behind this solution. Below those devices, you see cert 1, cert 2, those are Cisco IOS routers configured to run as PKI or certificate authority servers. To the far right lower corner, you see the spoke router, and it has the management tunnel with the security managed Gateway. Which in our environment we've used both the 3745 or in our larger environments, or our larger hubs, the Cat65K with the VPNSM and then now a VPN SPA. At the upper left hand corner in text, you see we have devices not on the management subnet that the solution relies upon. Known the ACS server for device authentication and then the provisioning infrastructure. This is incorporated into the existing enterprise management framework here at Cisco.

TYPICAL ECT DATA HUB

Here is a snapshot of our typical ECT data hub, it consists of two 7206 VXRs with NPE-G1 network processor engines. They each have an IPSec tunnel to the spoke router and that data is routed in a failover mode across those tunnels. To the upper left, you see the SDP registrar, or security device provisioning registrar, formerly the ECST registrar. In our environment we run on a Cisco 3725, but that could be any IOS-based device. And that comes into play only during the initial provisioning of the spoke routers.

ECT AND END-TO-END VPN

Here we have the ECT end-to-end VPN model that we like to describe as built on four pillars. And those end-to-end pillars are security, connectivity, deployment and management. And for most of the rest of our presentation we'll cover those pillars in greater detail.

END-TO-END SECURITY LAYERED SECURITY

So let's first take a look at end-to-end security, and the latest security features that can be deployed in an ECT environment. On the left, you see the features, the right benefits that can be derived from those features, and we'll cover those in the next slides.

RSA KEY LOSS DUE TO PASSWORD RECOVERY

First, we have RSAQ lost due to password recovery. Now if an Engineer or anybody attempts to perform password recovery on the router. What occurs is that the RSA private key will become unusable if the configuration is stored. If the user breaks into the router and tries to change the host name of the router, then RSA private key is permanently deleted. Now in either case, the router will not be able to establish a VPN session using the installed certificates without the private RSA key after password recovery. Essentially making the router useless for steps in the VPN tunnel.

PROTECTED PRIVATE RSA KEY

Next we will look at the protected private RSA key feature. In this instance, the RSA private key is actually locked by the password. It must be unlocked via this password in order to be able to be used to establish a VPN connection. VPN connections will not be established unless the private key is unlocked. This password can be set on the router when the router's initially configured. Now what this is effective anti-theft mechanism because even if the router is stolen. It cannot be used to establish a VPN session later unless obviously the RSA private protected password is known.

SECURE ARP

Here, we look at secure ARP and in this instance, the spoke router assigns an ARP IP address via DHCP that entry is actually secured in the ARP table. So an intruder cannot just get into the router and clear the ARP cache and use that IP address on their device to gain access to the Cisco network. Now secure ARP is an effective anti-spoofing mechanism. However, we feel the best approach for all services would be to require the devices to authenticate using device certificates.

AUTHENTICATION PROXY

Next, we look at authentication proxy which enables user authentication at L3 of the network stack. The user must authenticate in order to gain Internet access from their device, their PC workstation or laptop. And upon successful authentication, an access list will then be downloaded to the router from the AAA RADIUS servers to enforce corporate access policies. Now authentication proxy can be implemented in the mechanism to prevent non-employees from accessing corporate network resources in a teleworker scenario. And we refer to this as our spouse and kids solution for preventing unauthorized or non-Cisco employees from gaining access to Intranet resources. In addition, you could configure user access to different areas of our Intranet or your Intranet. And they can be controlled via the group information on the RADIUS servers.

802.1X-BASED DEVICE AUTHENTICATION

Another feature that could be deployed is 802.1x-based device authentication, it provides Layer 2 authentication of your network devices. And in our ECT environment, we intend to deploy two VLANs on the spoke router such as on the 87 series routers. There, you would have the trusted or corporate routable VLAN and the non-trusted or home VLAN. Devices that passed in the 802.1x authentication would be assigned to the trusted VLAN. And 802.1x has let's say, an advantage over authentication proxy in that it greatly simplifies the router configuration. Authentication proxy requires two additional extensive access lists, one, the intercept ACL and one a bypass ACL for devices such as IP phones. That do not perform authentication via authentication proxy; these accesses lists are eliminated with 802.1x.

CISCO IOS® CERTIFICATE SERVER SUPPORT AND PKI-AAA INTEGRATION

Next we look at Cisco IOS certificate service support and the unique Cisco offering of PKI AAA integration. Cisco IOS server or IOSCS enables us to configure a router as a certificate server. It supports certificate authority, remote authority and subordinate server modes. It also supports the feature of exportable and non-exportable keys and full backup and restoration of those keys. In addition, a unique Cisco feature of auto enroll is supported by IOSCS. And in this case, the endpoint is configured to try to re-enroll with the certificate authority based on a pre-defined expired lifetime of its certificate. In addition, IOSCS permits the storage of the certificates on external databases or on local flash of the router. In our ECT solution, we heavily relied upon PKI AAA integration which eliminates the need to manage certificate revocation lists. As a result, this significantly simplifies the management and deployment of a PKI solution and builds upon existing AAA infrastructure. What PKI AAA integration does is the spoke router presents a certificate to the hub router when it wants to establish the VPN tunnel. The hub router extracts the device name from the spoke certificate and presents that to the AAA server. If an account exists for that device, that information is returned from the AAA server to the hub router and the IPSec tunnel is negotiated. If an account does not exist for that device then that information is also returned and no further negotiation of the IPSec tunnel will be permitted. By eliminating the need of certificate revocation lists, you can have an immediate termination of a router. Rather than waiting for the 24 hour lookup that may be required when referring to CRLs versus an AAA infrastructure.

CISCO IOS® FIREWALL FEATURES

Now let's look at the IOS firewall features. IOS provides stateful firewall and context-based access control. The firewall ACL will block any access attempts from the outside. CBAC will then punch holes through return traffic for connections initiated from the inside. Now apart from the standard TCP and UDP protocols, CBAC also supports protocols like SIP, skinny, FTP, TFTP, among others.

INTRUSION PREVENTION SYSTEM (IPS)

Together with IPS, or intrusion protection prevention systems, which detect and attacks symptoms and raise alarms. It provides a very secure solution for our endpoints. First, IOS has an increasing number of built in signatures, over 100 as I speak. And new signatures can be uploaded to the signature device file on the router flash at any time. And combined with CBAC Cisco IOS-based IPS will perform deep packet inspection with a single lookup.

NETWORK ADMISSION CONTROL DEVICE POSTURE VALIDATION

And finally, we look at NAC, or network admission control, which provides for device posture validation. NAC ensures that only PCs with the latest anti-virus software can access the enterprise network. Well, in addition to anti-virus posture. It can check many other parameters like OS or OS patch level or other required software such as, in our network, Cisco security agent. These policies are configured on the Cisco secure ACS server, and each posture results in different network access levels for the PC. One caveat about NAC is that the anti-virus support or software on the PC must also support NAC. Today, supported vendors include Network Associates, Symantec and Trendmicro. Now I'm going to turn it over to Mike to talk about end-to-end connectivity.

END-TO-END CONNECTIVITY

Thanks, David. We're going to talk a little bit about the connectivity pillar and talk about the features underneath it.

DMVPN FUNDAMENTALS

Fundamentals, so DMVPN, or dynamic multi-point VPN. Is a Cisco IOS-based solution for easily building scalable VPNs by encapsulating GRE and IPSec. It relies on three proven Cisco technologies, IPSec, NHRP, or next hop resolution protocol. where that hub maintains a database of the spoke's routable public interface addresses. Where each spoke registers as routable address and the NHRP server after successful negotiation of the tunnel. And it also queries the NHRP database for routable addresses of destination spokes to build direct

tunnels. Multi-point GRE tunnel interfaces allow GRE interfaces to support multiple IPSec tunnels; it simplifies the size and complexity of the configuration.

DMVPN FUNCTIONALITY

Functionality, spokes have dynamic permanent IPSec tunnels with a hub, but not with other spokes. The spokes register as clients of the NHRP server on the hub. All routing information pushed to the spoke routers across DMVPN are via routing protocols. In a spoke to spoke scenario, when a spoke needs to send a packet to the destination, or private subnet on another spoke. It queries the NHRP database for the routable address of the destination spoke. The originating spoke then initiates a dynamic GRE tunnel and it's encapsulated in IPSec to the target spoke. The spoke to spoke tunnel is built over the MGRE interface.

ROUTING WITH DMVPN

So routing with DMVPN. Dynamic routing's required over hub to spoke tunnels. The spokes learn the private networks of other spokes and the hub via routing updates sent by the hub. From the hub perspective, the IP next hop for a spoke network is the tunnel interface for that spoke. It also has possible routing protocols, including EIGRP, OSPF, BGP and RIP. One of the features we have today enabled as EIGRP, and we have active failover. The failover between the spoke primary and secondary hubs occurs via this routing protocol, and in our scenario, the failovers less than 10 milliseconds.

DMVPN: KEY DIFFERENTIATORS

Key differentiators of DMVPN. DMVPN uses crypto profiles and tunnel protection, it frees the physical interface from a crypto map. Management's performed over a separate VPN tunnel independent of the data primary DMVPN tunnels. It allows for dynamic registration of spokes where one tunnel interface is defined on the hub and it spokes a single DMVPN cloud. It eliminates static point-to-point configuration and reduces the complexity of the hub configuration. DMVPN provides dynamic full and partial mesh capability and it provides improved support for applications such as voice and video.

IP APPLICATION SUPPORT

IP application support. IP phones are supported, both SIP and skinny. QoS for VoIP is provided on the spoke routers, with LLQ and shaping. It provides acceptable voice for links with generally speaking greater than 128K upstream bandwidth, but in our implementation we recommend 256K. Future improvements will allow QoS settings to be applied per security association from the hub. It also supports multicast, can support video, and in future phases for our implementation, will support managed Wi-Fi with the 871 ISR router.

END OF PART 1

This is where we end part one. If you'd like to see how we deploy several thousand routers to our employees' homes using something we call zero touch deployment. And how we manage this extended router network, you could click on the part two URL just below the part one URL on the same page. We hope to see you there.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco.com Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA C78-337358-00 02/06