12 VPN2 – VPN Part 2

Hello, and welcome back to part two 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 at 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 two, we focus on how we deploy and manage the hardware VPN solution and some of the tools we use. We'll follow-up with a short Q/A session and show you how, where you can find more resources.

HARDWARE VPN AGENDA

On the agenda, we're going to pick up with the model and talk about end-to-end deployment, end-to-end management and then finish with best practices. I'm going to turn it over now to David Iacobacci who's going to talk a little bit more about deployment and management.

AUDIENCE COMMENT: Thank you, Mike.

END-TO-END DEPLOYMENT

So here's a list of the features and components of the deployment pillar in our ECT model. First, we'll cover conventional provisioning of CP spoke routers, and we'll look at three deployment options we implemented in ECT. Delving into details of zero touch deployment giving you an overview and then breaking it down into two parts, secure bootstrapping, secure policy enforcement. Then we'll go through a step by step process of how a router is configured using the zero touch deployment model. We'll cover one other deployment option in detail, that is the online or cert proxy method and then give you an overview of zero touch deployment of an IPT device for remote access.

END-TO-END DEPLOYMENT MAJOR FEATURES AND COMPONENTS

Major features and components of our deployment model include ZTD, the zero touch deployment, which is it touches an automated configuration of our remote devices. We rely upon secure device manager, or actually formally Cisco router web setup tool, CRWS, which is a GUI interface that allows the user to configure an IOS device to gain network access as part of the zero touch deployment solution. We also implemented secure device provisioning, or STD, formerly EZSTD, and this securely bootstraps routers including enrollment in the PKI certificate server that is used to authenticate devices as part of our management tunnel. Then we also have IP solution center, or ISC, which is used to securely provision and audit our spoke routers. And we also use IE2100 intelligence engine, which is the muscles of our solution, and it is the CNS transport engine that we implemented to use for the CNS transport services in our network.

CONVENTIONAL PROVISIONING AND DEPLOYMENT OF CPE/SPOKE ROUTERS

Now in the convention of provisioning deployment of spoke routers, we had three models that we used in the past. We had the in-house model where the router was configured by an IT Engineer. Five years ago we had 12 Engineers, just in San Jose alone, configuring ISDN and frame relay routers for our employees. Another model would be to outsource the router configurations to an ISP where the ISP would be responsible for ordering the routers and they'd be shipped to the ISP staging facility where the routers would there would be configured before then being shipped to our employees. And a third option would be to outsource to a third party, and there the router could be configured at a staging facility or even onsite at our employee's home. But all three models add excessive cost to the deployment process as

an Engineer or technician must open the box and touch each router, and then, in most cases, send it on to the employee. The key to our ECT solution was then how to minimize the amount of experts that have to touch the router.

ECT OFFERS THREE DEPLOYMENT OPTIONS

ECT, we have three deployment options, ZTD, where first the user's responsible for configuring the router for Internet access and then running EZSTD. Then after the management tunnel is built as part of the process of EZSTD, then policy configurations are pushed to the router configuration over the CNS transport mechanism. Our second method was online or cert proxy which allows the Engineer to access the router remotely over the Internet and paste the configuration information as required in it. A third option was our offline, where, this was for special case of situations or in our pilot environments. Now regardless of the deployment option, the spoke router provisioning process was automated as much as possible to minimize the TCO.

ZTD STEPS

Now ZTD can be broken into two steps. You have the secure bootstrapping, which is with configuring the router with enough information to establish the management tunnel and limit access to devices on the management subnet. Then, over a CNS connection would be established from the router to the IE2100 and ISC, configured information would be pushed to the router. The second part is does that with that configuration information would be pushed to the router and then the router would have full access to internal network resources as per the enterprise guidelines.

ZTD SECURE BOOTSTRAPPING

So let's look at secure bootstrapping, it involves configuring the router to connect to the management Gateway. The bootstrap configuration includes Internet connectivity, which the user already should have established using CRWS or SDM. And in enrolling the router in the PKI certificate server that would be used to authenticate who's certificates would be used to authenticate the IPSec management tunnel, and then the CNS agents would be configured on that spoke router. Now in CNS, the spoke router is the CNS agent, the IE2100 is the CNS engine, which is basically the in-between between the agent on the spoke router and IP solution center, the CNS server. All CNS traffic via from the spoke to the ISC, or vice versa, has to transverse the IE2100.

ZTD SECURE POLICY ENFORCEMENT

Now secure policy enforcement occurs when the ISC server receives a CNS device connect event from a spoke. It will then push the states configlets to the spoke via the IE2100 CNS engine. Now policies are actually represented as configlets, which are generated by service requests on the ISC. And in our ECT phase 1 deployment, the policies that we started with were DMVPN IPSec, firewall, QoS and NAC. Our plans include through our policies for 802.1x, NAC, IPS, NBAR, and others as required.

ZTD OF A SPOKE ROUTER: STEP-BY-STEP

Now here is a step by step breakdown of the zero touch deployment model of our spoke routers. In step one, the user would apply for the ECT service, and after their manager approves their application, the user orders the router from cisco.com. In the meantime, templates and service requests are auto-populated on the ISC. Router is then shipped from the factory to the user and when the user receives the router, they connect it at home to their ISP and configure it to gain Internet access using CRWS or SDM. And from a device behind the EZCT router, the user brings up a browser and establishes an SSL session with the EZSTD registrar at the data hub. In that process, the router is enrolled with the certificate server who's certificates are used to authenticate the management tunnel. And also CNS connection information is configured on the router. That point, the IPSec tunnel to the management Gateway is established with a successful authentication from the hub using PKI AAA integration. And the CNS agent on the spoke router sends a connect event to the IE2100 CNS agent at the management hub, and it proxies that connect event to the ISC server. At that point, the ISC server then pushes all policies and configlets and templates, earlier we spoke to the DMVPN IPSec, the firewall, NAT and QoS, and actually enrolls the router in the

certificate authority who's certs are used for authenticating the data tunnels. That point, the data tunnels should be established and the spoke router should have both primary and failover data connections to the hub routers.

ON-LINE DEPLOYMENT (CERT-PROXY)

Our second deployment option is cert proxy, or the online method. And cert proxy is a tool in ISC that allows ISC to authenticate and enroll in a Cisco IOS-based certificate server on behalf of the router. Now the user must still configure the router to access the Internet in this scenario. And upon gaining access to the Internet, the Engineer should be able to access it remotely and actually paste the certificate and configuration information required to bring up the management VPN tunnel in the user's router. The remaining configlets that are the service requests from the ISC are pushed to the spoke router upon establishment of that management tunnel via the CNS connection over the tunnel.

ZTD OF IPT FOR REMOTE ACCESS

Now let's just look at our zero touch deployment option for IP telephony devices in a remote access environment. Here again we'll go step by step. The user would apply for the IPT service as part of the ECT service in our plans. Upon their management approval, they order an IP phone or install IP communicator on their PC. At the same time, an additional instance of a phone is configured for their employee's dial number, or DN, on the Cisco CallManager. The IPT device is meanwhile shipped from the factory. The user has then configured their router and established data tunnels with the data hull, the user then connects their IPT device to the ECT router. CNS agents on the router sends a cns.ipphone.connect event when the IP device is actually connected to the router, and that event includes the IPT MAC address, the host name, and the IP address. And this event is then published by the IE2100 CNS engine on the Tibco bus, which is a logical bus, that CNS can be configured for CNS servers and engine, the IE2100 to listen to. A Java agent listens for events on the Tibco bus and intercepts that specific event, the cns.ipphone.connect event, and associates the MAC address information with the DN in the CallManager. At that point, the TFTP session is established with that IPT device and configuration information is sent from the CallManager to the IPT device.

END-TO-END MANAGEMENT

Next, let's take a look at end-to-end management. We will take a look at the basic functionality of a ISC and then take a look at the policy management GUI that it offers. Then we'll look at a snapshot of its GUI for CLI commands, ACLs and enable secret password rotation before turning our attention to the IE2100 and its basic functionality. Then we'll look at its GUI that we use for image management and then the GUI for log management. Finally, we'll take a look at how we designed the data inputs, how we integrate into our existing enterprise management framework at Cisco.

ISC BASIC FUNCTIONALITY

Now IP solution center version 3.2.2 that we use at Cisco supports the following basic functions. It can be used to create and deploy and audit policies, and the ones we've used, as we've told you, the IPSec DMVPN, the firewall, QoS and NAT. It can also be used to create and deploy velocity-based templates and instantiate these templates with data files to create configlets during the deployment. Now the difference between templates and service requests are that ISC actually can audit configurations that are pushed from the service request. Templates will be put, template information to templates, is pushed to the router configuration, however, ISC has no way to audit that if it's changed at a later date. ISC can also be used, as we do, to change CLI commands on the routers in the configuration mode, the ACLs on the routers, and also to rotate or enable secret passwords. ISC communicates with the IE2100, the CNS engine, over the Tibco bus to push and pull policies, and these policies can be event-driven, such as a CNS connect event, schedule-driven, time of day, or rapid deployment immediately. ISC also supports XML SOAP interface and has an extensive library of northbound APIs enabling integration with an existing enterprise management framework. ISC also offers the fully managed service or FMS functionality, which notifies administrators of non-ISC initiated configuration changes to the policies pushed as part of the service request.

ISC POLICY MANAGEMENT GUI

Now here is a snapshot of the policy management GUI on the ISC. Here we have one spoke router with four service requests, the NAT QoS firewall and IPSec, in different states of deployment. We have the wait to deploy where everything is ready for the CNS connect to be pushed information so that configlet can be pushed to the spoke router, and the others are in a state waiting for it to be instantiated with the data from the data files.

ISC ACL/ENABLE SECRET MANAGEMENT GUI

Here's a snapshot of the GUI that we use to push configuration commands, ACL changes, and rotate enable secret passwords. This is the device console feature in ISC. You have a spoke router that has been selected or you could select a group of routers, depending on how you've grouped them in your ISC. And then you have the actual commands that are shipped down to the router; they are changing the enabled secret and a standard access list. Upon hitting the submit button, in this window, the commands would actually be pushed to the spoke routers and then you would see a report, success or failed based on if the device was reachable over the CNS mechanism.

IE2100: BASIC FUNCTIONALITY

Now the IE2100's basics functionality supports the following main CNS agents. The event agent, which enables the CNS management; it actually sends the connect and disconnect events to the ISC on behalf of the spoke routers. Then there's the exec agent, which allows remote applications, in our case the ISC, to send CLI commands to the router. And there's the partial configuration agent, which allows configured push, pushes and notifies the ISC of unauthorized configuration changes to the policies that it's pushed. And then there's the image agent, which enables image upgrades over the management tunnel, of course being initiated by the CNS mechanism. Now the IE2100 supports the following basic functions; it can be used to push or pull policies, CLI commands or populated templates. It notifies all subscribers on the Tibco bus of the events originating from the CNS agents, such as config change, load, warning or others. It generate and sends to all Tibco subscribers two events, connect and disconnect, on behalf of the CNS agents on the spoke routers. We use it to perform IOS image management, and in version 1.5, they offer a significant enhancement and that is the ability to create and deploy, again, velocity-based templates. These templates can be instantiated with data files to create configlets for deployment, and these configlets would be staged, again, ready to be pushed to the router upon a CNS connect event. IE2100 also provides the capability to perform upgrades and updates based on schedules, event-driven or rapid deployment. This is very important in a remote access environment where often the spoke router is not connected, as opposed to routers on the corporate network or devices on the corporate network where they're always up and normally reachable via features such as SNMP.

IE2100 IMAGE MANAGEMENT GUI

Here's a snapshot of the image management GUI on the IE2100. Here you have spoke routers, and what you would do is would be to click on it, specify the image you want to be downloaded. And you have the options of check the images there already, and if it's there already, push the image or not, to do a check on being successfully downloaded to the router, among others. Now this image would then be pushed across the management tunnel from the server specified in your IE2100.

IE2100 LOG MANAGEMENT GUI

Here we have a snapshot of the log management GUI also on the IE2100, and you can see different messages with different spoke routers, which is connect, warning, config change. This is just some of those that you would see, and you could further refine your view in this to specify specific strings, such as a specific spoke router. It can be a powerful tool when you are troubleshooting issues with one network device or several.

ENTERPRISE MANAGEMENT FRAMEWORK INTEGRATION

And here is how we design the data in the ECT solution to integrate into our existing enterprise management framework. On the upper left, you have the user zone, this is information provided by HR or the user when they register for the service. The middle top, we have the client zone, most of this information comes from EMAN, as shown in the bottom left hand corner. Other information comes from other components in the ISC solution, such as the security management Gateway, their hub, cert number, etcetera. The upper right is the ISP zone, this information is also provided by the user upon registration. It includes how the device or how the spoke router obtains its IP address on its outside interface, DHCP, PPPoE, or static, and any information related to that, such as PPPoE, user name, password, etcetera, and the NS server among other items that may be necessary. Now turn attention to bottom left is the AAA zone. Now this is where we have information for the device, the end router's AAA account on our ACS servers. Moving to the center there, we have the policy zones. This is basically what we started out initially with the four policies, which we'll expand in later phase of the IPSec, firewall, NAT and QoS, and which ones this spoke routers subscribe to on the ISC. The information from ISC is then shown into the management tool. And finally, on the bottom right hand side is the operational zone, and this is information that EMAN collects, they're our enterprise management framework, collects and gives a once view for the network Engineers on the current status of the spoke router and it's connection into corporate.

BEST PRACTICES

So best practices, things we learn by rolling out ECT. First, start with a limited pilot and become familiar with the technology, understand the information requirements and the system flow. Plan a phased approach for these services. Start with data and then migrate to other services like voice, Wi-Fi and video. Automate as much as possible for your production process, that includes everything from the user phase, all the way to the provisioning phase. Select hub locations to optimize latency for most users. In our case, what we do is we looked at where the population resides. So we look at population density, we also look at where we have our ISP links in our network externally. So those are some of the things we learned, and we hope that you can benefit by them.

SLIDE 22

So we've put some questions together that customers have asked us about this topic in previous sessions. We have a little time left and I'd like to take this time to answer a few of them. Cisco IT's used ECT as a remote access solution, but what other models are possible for solving customer problems?

AUDIENCE COMMENT: Well, we've looked and we've talked to customers who would like to use an ECT-like solution for their branch office network. And examples would be like a large integrated oil company where the branch offices are the gas stations themselves, or financial customers where the bank branches are the endpoints in a ECT-like solution. Great, so VoIP is a big business driver. Let's talk about some of the best practices Cisco uses internally for remote VoIP.

AUDIENCE COMMENT: Well, we take a number of steps to try to maximize the quality of the VoIP experience for our users. First, for all remote telephones, we ask that the CODEC be set to G.729, which is a low, requires much less bandwidth than the standard office CODEC of G.711. Second, we asked our clients to have a minimum of 128K kilobit per second upstream bandwidth, but we really encourage them to have 256K kilobit per second or more. Third, on our spoke routers, we deployed a number of class map policy maps, and if necessary, traffic shaping, which should result in customers having, we'd say, about 95% or greater of their time their VoIP is office quality. Thanks, so beyond setting up infrastructure and initial deployment, what other downstream network components are important for considerations for deploying a hardware VPN solution?

AUDIENCE COMMENT: Well, with ECT, we're riding on our ISP connection, the information ISP connections into the corporate net, so obviously we have to work with the teams that manage those and our DMZ. In addition, because VoIP is one of the first services people

want to use over this solution, you have to work closely with our teams that manage our telephony infrastructure, make them aware of it, and we have to work together as it is a service to the users. And they're not going to ask, it's a problem with the router or it's a problem with my phone, it's a problem with the service. So really it's your ISP Gateways making sure you have enough bandwidth, it's really making sure that you have integration with other service teams within IT, and it's also making sure that the users understand what the service is and what the limitations are.

AUDIENCE COMMENT: That's right. Okay. ECT's an extension of the corporate network in the home. Let's talk about scenarios to limit support for non-corporate assets and ways we can securely permit and route home PC traffic over this solution.

AUDIENCE COMMENT: Well, we talked a lot about authentication proxy. So the user, in order to access internal resources from their device, has to actually authenticate, otherwise their traffic will be routed to the Internet for other items, public Internet resources. In our model, you could rollout the solution as split tunneling enabled where all traffic not destined for the internal organization Intranet would be routed right out that spoke router internet, or you have non-split tunneling where all traffic is first sent back to the corporate headquarters or, excuse me, the data hubs, and they would then route that back out to the internet as necessary. Okay. In later phases of ECT, we look to employ 802.1x and to minimize potential effects on the internal network NAC or for device posture validation. Right, so really it's an area where we have, typically IT doesn't want to go towards the home because they don't want to support the home network. Absolutely. But we have the ability to do some demarcation, so we have the ability to support that home traffic, as well as make sure it's secure so only corporate traffic can be routed back to the corporate network. Yes. Great. I'm afraid that's all the time we have for questions today.

MORE NETWORKED HOME/ACCESS RESOURCES

And for more information about Cisco IT deployments, you can go to the Cisco IT at work site to find Cisco IT case studies about what we deploy, what benefits we've gained, what lessons we've learned, and some operational practices and presentations to help you learn more. You can also find more information on security VPN, design guides, operational practices and several other documents, white papers and presentations on cisco.com. Below that, you'll see a toll free number you can call for more information or to place an order. You can order Cisco resources on the web from the URL at the bottom of this page.

SLIDE 24

I'd like to thank those of you for watching and spending this time with us, and being interested in what global technology seminar series is all about. We hope you've enjoyed the show and that it's helped you answer some of your questions about VPNs in general, and hardware VPNs, in particular. And thank you, David, for spending and sharing this time with us and your expertise and enthusiasm for VPN access services.

AUDIENCE COMMENT: It was a pleasure, Mike, and we hope that you've enjoyed the show too. See you soon.

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 C78-337360-00 02/06