Security at Cisco – Part 1

Hello and welcome to the first of a two part “Cisco on Cisco” seminar on security at Cisco. I'm Rich Gore, Manager of the Cisco at Work Team which is a part of Cisco IT's Cisco on Cisco initiative. The theme of our show today is going to be security at Cisco. It'll be an overview of how security fits into the overall philosophy of Cisco and a tour of a lot of the different technologies that Cisco uses to support security in our business network environment. We'll review some of the security policies and procedures and some of the technologies that support those policies, then we'll take a quick break and come back to finish up our security technology review and also to share with you some further resources. Now it's my pleasure today to introduce the star of today's seminar on security at Cisco, both parts, Laura Kuiper. Laura has been with Cisco, with us for eight and a half years, first as a Cisco IT Network Engineer, then as an Information Security Engineer and then most recently as a Consulting Security Engineer within the corporate development consulting team. So Laura I want to thank you very much for coming today. Thanks Rich, it's a pleasure to be here today and to be able to share with everyone some of the information about how we do security here at Cisco using our own products and technologies and features that we have in them. This is an area that's especially interesting to me so I hope it is to you too, so please sit back and enjoy as we explore some of Cisco's security capabilities.

AGENDA

So first off we're going to start with the agenda and the first thing we want to do is set the stage for who is Cisco so everyone understands what we believe is important and what we're looking at securing. Next we're going to look specifically at the security technologies that we're using; we'll do a review of what the technology is and then how we're actually using it here at Cisco. And then lastly we'll summarize with what is the summary about, why security is important and then what we're going to be doing going forward and some references. Excellent.

CISCO SECURITY COMMITMENT

So the first thing is that we have a commitment from our senior management to have Cisco at commitment for security from the top down. John Chambers our CEO has stated security starts with me the CEO down to the individual contributor level, it's mandatory, it's not an option, security's part of everyone's job and it's important for everyone to have security. That's a very high level endorsement. I'm thinking about the companies that perhaps don't have that kind of strong high level endorsement. Do you think Cisco has it easier, at least in the information security space because of John's commitment to security? Absolutely, I think that because of John's commitment to security it makes it much easier for InfoSec to be able to have policies and procedures that include everyone, and help everyone understand that security's not just InfoSec's job, it's everyone's job.

SO, WHAT IS SECURITY…

Good point. So what is security? One of the things about security is that, one size doesn't fit all. The reason that we're starting with who Cisco is that what's important to Cisco may not be important to the next company. Security's important to everyone but it doesn't mean that everything we do is right for everyone else. So what's important to an organization we have to find and then deliver it to make it highly individual and highly successful? Security decisions are really business decisions based on what the business model is and what's important. So we have to understand the overall direction, the business model and our culture to be able to understand what's important from a security perspective. Security decisions are really business decisions but I just assumed security was making sure stuff doesn't get stolen. Security goes beyond just stuff being stolen. Okay. When you have to look at what's important to Cisco, our source code for

example, that's something that's very important to Cisco to secure because we don't want that to be stolen. However, let's say you're at another company where maybe they're doing movies, so for them securing that movie information is going to be important and that's what the business driver is, they're making money by doing that. So the security choices that they're going to make are going to be because their business has certain needs. So we'll be protecting the source code more strongly than we'll be protecting, say, this particular video. Absolutely. Okay, makes sense. That would be type of information.

SO, WHO IS CISCO?

So who is Cisco? We are over 38,000 employees. We have over 10,000 contractors, so part of it is the people themselves. We have multiple systems, you can see we have thousands of systems and various types. We have information that is both our assets, as well as customer information. So for us securing our source code is important but also securing our customer information that we have stored is just as important because we've made a commitment to make sure that that information is secure. In addition, we want to keep productivity high and we have eight primary Internet connections around the globe, not including some of our secondary connections. We have over 900 labs around the world and those continue to grow. Trying to protect the labs as you're trying to do new work is very important, so we want to make sure we keep those labs safe but allow them to continue to work. As you can see from this information, we've got a lot of different areas that we're trying to protect and a lot of different ways that we're doing the protection. So a couple of questions, primary versus secondary Internet access points. What's the difference between a primary and a secondary one? So from a primary standpoint, our primary ones mean that all of the Internet traffic, both from me browsing the web on my desktop, to somebody coming in via VPN, can come through that connection. A secondary connection is, we have found that there are certain places around the globe where it makes sense to have a VPN connection for people locally in that region to connect directly to. So local VPN-only secondary. That's absolutely correct. Okay, okay. And 1,000 labs? We have quite a few labs. We are a company that's made to be doing research and development, to do research and development you have to have labs. Is that a particularly difficult thing for security to work with? It's extremely difficult for security to work with because you don't want to hinder and this goes back to the business, you don't want to hinder the ability to make new products but at the same time you've got to protect the rest of the company to be able to do its job. So you have to control it but keep your hands off at the same time. Absolutely and that's a balancing act that InfoSec has to work on a regular basis. Okay, thanks.

CISCO CULTURE

So one of the other big things that we said was culture makes a difference on how you look at security. Cisco culture is really one that's based on employee trust; it's got a biasness toward openness. We want people to be trying new things; we want them to continually evolving products and features that we have. We embrace the virtual company model which is very important moving forward because we're so global. We also implement bleeding edge new technology. Now we say bleeding edge because sometimes you're staying awake long nights and you get bloodshot eyes with waking up, so you have to be aware of that as well. Because sometimes you don't know what's going to happen and so you have to be aware of what the security implications are of something that you're unfamiliar with. So the way Cisco's InfoSec actually approaches this is we preserve the openness by lowering the risk. We look at, what can we do to lower the risk but still allow you to continue to do your job. We build awareness consistent with the culture. As with John Chambers, it comes from the top down, security's not only InfoSec's job, it's everyone's job. And they have proactive involvement in new technology deployment, so InfoSec's involved in talking about new technologies, how do we include security. In consulting security engineering what I'm doing we also work with the new products with, how do we put security into our products from the beginning rather than as an afterthought. Control's only when necessary. So like with labs we only put the minimal types of controls that are necessary. How do we protect with anti-virus? How do we limit that type of access from the labs to our corporate network, but still allow them to be effective? And lastly we do have employee trust. We monitor and we verify we don't just assume everyone's out to get us. Okay, so I can see the balancing act starting to take shape here. Absolutely, it's a big balancing act and InfoSec has a lot on its plate doing that.

WHAT ARE THE CONCERNS?

So what are the things that we're concerned with? So now we've talked about what it is that Cisco has and how we're looking from a business model how to do security. What are we trying to protect? Well, one of the big ones is we're trying to protect against disruption. Disruption is loss of productivity. This might be a problem with somebody has a new bleeding edge technology, it fails, what happens to the rest of the network? Somebody tries to break in or they deface one of our websites, this would all be disruption. Loss, loss affects the value. What is the value proposition of our source code, how valuable is it, we want to protect against losing that value. It's also valuable to Cisco to be a trusted security advisor. So from a security perspective we consider security a value, so it's important to continue evolving what our security best practices are. And the last one is damage that affects reputation. So damage would be simple things as if a CCO got defaced. This affects the reputation of the company; it affects the reputation of being a trusted security advisor. So these are the three main areas that we look at from, what are we trying to protect? We're trying to protect against disruption, we're trying to protect against loss and we're trying to protect against damage to our reputation.

1. SECURITY STRATEGY: PROACTIVE & REACTIVE

So the question will become how do we do that? An excellent question, Laura, how do we do that? So we actually do that, we have both proactive and reactive ways that we do this. And what we're going to do is through this next section, we're going to talk about the technologies we're using to do proactive and reactive methods for each of the areas, for disruption and loss, what are we doing. By protecting against both disruption and loss, we can protect against damage to the reputation. Makes sense.

2. SECURITY STRATEGY: PROACTIVE & REACTIVE

So the first area we're going to talk about is anomaly detection and DoS protection, DoS being denial of service. So the two areas that we look at here, we're going to look at Arbor and Netflow for anomaly detection and we're going to look at the Cisco Guard on what we use for DoS protection, so these are either Cisco technologies or partner technologies that we're using to protect ourselves.

NETFLOW PRINCIPLES

So what is Netflow? So first let's talk about what the technology is. Netflow is typically considered is inbound traffic only. Luckily, with IOS 12.4 we were able to now do egress Netflow as well. So not only looking at traffic that's flowing into the router, we can look at traffic that's flowing out of the router and get a real good picture about what's going on. The nice thing about Netflow it accounts for both transit traffic which means it doesn't have to be destined for that router, it might be destined for three routers down the road but we can see what that traffic is. So we can also do traffic monitoring going, how much web traffic do we have, how much instant messenger traffic do we have. All of those can be looked at through Netflow. So what sort of information does Netflow give you? It gives you how many flows and how many packets are coming through across the router. Now what's useful about that is there's a typical amount of traffic that you expect and from Netflow you can look at how much of that traffic am I seeing. When you have a DoS attack for example, Netflow can tell you information about, oh look I'm seeing a lot of one packet flows, which are very unusual, coming through from this source to multiple destinations or from multiple sources to a single destination. That will quickly key you that you may be having some type of DoS attack, so you use this in conjunction with some of the other products like the Cisco Guard. Okay, thank you.

KEY CONCEPTS

So what are some of the key concepts about Netflow? You can think of Netflow like a phone bill, it tells you, start it here, end it here, how long did it go, how much traffic went across it? You know how a lot of the times now hotels charge you if you use their phone lines to actually send data across, they'll charge you for how much data you sent or how long you were online. Netflow can do that from an IP standpoint as well. The other thing about it is that it gives you great telemetry, like I said, with regards to DoS attacks. The advantage of Netflow is, it's in all of your routers, it already exists in there, which means that you can take advantage of it, you do not have to add anything new. Once you turn it on, it doesn't impact your router. What it does is it allows you to be able to look at the information on a

regular basis. You can actually look at it directly on the router as well as having it offloaded to a third party system. What we at Cisco do is we use Arbor, which is a partner product that takes the Netflow information and makes pretty charts for us.

TRAFFIC GRAPHS

So suppose I'm a network administrator and I want to see if there's been, say a 25% increase in traffic going through one particular router in a span of five minutes, or some parameters like that, will I be able to get an alarm for that if something like that happens? So using a product like Arbor, you absolutely can, you can set certain thresholds. One of the things that we use as an example is, during SQL Slammer, which was back in 2003. I remember it, yes. However, we were able to quickly find out that that was happening because we set threshold alarms on Arbor. The chart here as an example shows you where we actually saw that. You could quickly see from this chart that there was absolutely a problem. Yes, there's certainly an anomaly there. We saw that it was port 443. At the time, we did not know what that was but we knew that we needed to react to it because it was an anomaly, and so we were able to protect ourselves with SQL Slammer and we used a large part of that was done through using Netflow and Arbor together. So it looks like there was this huge spike of traffic. Is that inbound traffic coming at the bottom? That would be inbound traffic coming from the Internet. And then it gets choked off relatively fast and then choked off more and more slowly over time. Right, so the reason it gets choked off more and more slowly over time is because there are still people sending it from the Internet, so this would be from our Internet Gateway. We didn't get affected because we blocked it coming into Cisco's internal network. It slowly decreases over time because more people on the Internet started cleaning it up. Choking that traffic back. Absolutely, so you start seeing less of it coming towards you. Makes sense. So that's why it slowly filters off but you can quickly see that we saw a large spike, and that's how we knew what to react to. Makes sense.

1. CISCO GUARD

So the other product I want to talk about today is going to be the Cisco Guard. Now the Cisco Guard is a product that we actually got from Riverhead and what's really nice about it is it allows you to do mitigation of DoS attacks and it does it in such a way that you don't have to worry about the good traffic being blocked. So when you do a regular black hole and you're doing black holing of traffic, you can't get any traffic then to your destination. One of the things the Cisco Guard does is it still allows traffic to flow that's classified as legitimate traffic. It filters on that traffic; it has learned what's normal and what's not, so it's an auto baseline rather than a signature-based system. Auto baseline, I think I understand signature-based, that sort of means like a virus signature, or in this case, a worm signature. What does auto-based mean? What auto baseline is, behavioral or learning, it's going to learn what normal traffic for your network is. So that's one of the things this will do is it will discover what are normal services, what is a normal amount of traffic, identify HTTP proxies that are normal. It will identify all of this and know then traffic coming from those particular types of things going to a particular service destination is very normal. And then when something happens that's an anomaly, it'll stop that traffic but allow the normal traffic, what it classifies as normal traffic, to continue to the destination. So what happens when like Cisco puts in completely new gear, which we actually do kind of frequently,

2. CISCO GUARD (CONT.)

that does something completely different and different types of traffic flow to a different address on a different port, does Cisco Guard figure that that's bad traffic and block it? Because Cisco Guard is not inline and it's only triggered when we notice an anomaly, then it can learn about that traffic before you have an anomaly. Does it run and ask somebody? Does it say, hey, there's something going on here? It actually goes and it talks with Arbor, it will also talk with the Cisco detector, it will talk with a manual system, so you could do it manual, so there's automatic and manual ways to do it to allow you. So let me step through how it actually works.

3. CISCO GUARD EXAMPLE

So the first thing that happens is it detects that there's a problem. So maybe Arbor said, oh wait, look, I have this anomaly. What happens then is it lets the Cisco Guard know, so my Arbor system will let my Cisco Guard know, hey, by the way, we've seen this anomaly.

4. CISCO GUARD EXAMPLE

Send the traffic to you so you can scrub the traffic, and allow the clean traffic through. So it sends a BGP announcement to the router, that's actually how it's going to communicate to say please send me this traffic.

5. CISCO GUARD EXAMPLE

So it diverts only the target traffic and in this example you'll notice there's a set of servers that are our target and there's another set of servers that's not the target. The only traffic being diverted is the target, meaning whoever's being attacked.

6. CISCO GUARD EXAMPLE

What happens then is it'll identify and filter out the bad traffic. So it knows what the good traffic is and it says okay, this is bad traffic, I don't want to allow this through, but I'm going to go ahead…

7. CISCO GUARD EXAMPLE

…and I'm going to allow the legitimate traffic, so it'll then forward the legitimate traffic back to the target. So for example, if CCO were under attack and we used the Cisco Guard we would be able to filter out traffic, people would still be allowed to place orders as legitimate traffic without having their ability to place orders impacted. That's impressive, before Cisco Guard was in place what did we do?

8. CISCO GUARD EXAMPLE

I mean, I'm sure that Cisco might at some point have been under attack, what would we have done without Cisco Guard in place? Without Cisco Guard in place we would have actually used ACLs to actually do that. We would have looked at some traffic and we would have said, okay this is what we consider bad traffic coming in. Netflow has been around a long time and so we would have used Netflow to identify what that traffic was. The biggest thing is that we've seen an increase in the number of DoS attacks and that's where the Cisco Guard has been able to help us quite effectively. Because it's automatic, it happens very quickly as opposed to someone having to go in and type in the new ACLs into the router. Correct, that is correct. The other thing is that with the Cisco Guard it doesn't have to be automatic, we can do it manually, so depending on what your level of trust is for automatic systems would determine that as well.

AT CISCO: ANOMALY DETECTION & D/DOS

So what are we using here at Cisco? For anomaly detection and DoS attacks, we do use Netflow. We have Netflow deployed on all of our network edges, which means all those eight primary ISPs we've got Netflow all out there. We have Netflow in some of our internal networks as well so that we can look at internal traffic. You'd be amazed at how many times we've seen internal DoS attacks attacking ourselves without even knowing it; this is where we have to be concerned with the labs. I'm curious now, internal DoS attacks. So somebody like me brings in our laptop and we unleash a worm, is that? Absolutely, so sometimes people will do that. You connect at home, you're not connected via VPN, maybe your anti-virus isn't running and all of a sudden you've got a worm. You come into the office, you plug into the network, you could potentially have that happen. That happens quite a bit in the labs, which is why we were concerned with anti-virus there and why we're trying to help work with them finding a solution. Arbor Peakflow's what we use on the net edges to identify DoS attacks and anomaly detection. As I said, Netflow's also deployed internally. We use NetQoS, which is another product that also uses Netflow, we use that for capacity planning and anomaly detection internally. So Arbor's used on all of our external edges, all those eight primary ISP locations, and NetQoS is used internally to be able to look at traffic patterns. Because you'd be amazed how many field sales offices have unusual traffic patterns that may mean that we need to make a larger link. That makes sense, for capacity planning that would be critical. For capacity planning, absolutely. And then we use Cisco Guard, and we're using Cisco Guard with both Arbor and the Cisco detector to actually mitigate DoS attacks. So for Cisco we're using all of these because we find that they're very useful and we're able to actually mitigate a lot of the security concerns that we have. Makes sense.

SECURITY STRATEGY: PROACTIVE & REACTIVE

So the next area that we're going to talk about is we're going to look at, what are we doing from a scanning and intrusion detection perspective, what are we doing for our syslogs and how are we doing traffic analysis, other analysis.

CS-MARS TECHNOLOGIES

So this is an other than distributed denial of service attack, this is a more subtle intrusion you're looking for. Yes, this would be just more subtle, this would be your viruses and your worms. This would be somebody trying to hack in, so that's where your IDS is going to actually come into play. Makes sense. So for again, first I want to talk about some of the technologies. One of the new technologies that we have is called CSMARS. Now CSMARS is Cisco secure MARS and again another acquisition that we've done. The nice thing about Cisco MARS is it takes a lot of information in; it'll take Netflow information, syslog, IDS, it'll all feed it into a central engine. What it does then is it takes that central engine and it basically funnels it down to useful information because if you look at the number of syslogs that we get, you could look at those and be totally overwhelmed. So CSMARS will actually help you correlate information. Oh look, I saw this on the syslog, I saw this on the IDS, and I saw this in Netflow, so I can quickly correlate and say, oh, you might have a problem. So CSMARS receives and monitors all the events, so it's event correlation. Now I've heard stories of earlier IDS systems that would filter out 50,000 alarms and reduce it to only 5,000 alarms, which would still be overwhelming for a team of 10 people pouring through them day after day. To what degree does CSMARS reduce that load? It reduces it even further by doing more correlation. So it realizes that if it saw it come in on the IDS maybe outside the firewall but it didn't see it come in on the IDS inside the firewall but it saw a message on the firewall that said, oh look, we blocked this, you could see where that might be leading. So you're able to actually tune it, is what they call it, tune it to a better level, so that's where CSMARS can get you. It's very rapid, it's inline so it's very quick to process these events and it focuses on validating the events, so that's all it's doing. It's not going to go in and investigate the events, it's going to provide you a report that says, here's the events you should go investigate. So that's one of the areas where process and policy come into play, how do I process those, what's the process of validating it once I actually look in it, so I go in and investigate it. We're going to talk in a few minutes about incident response, which is going to be how do I actually do something with an event that I did find, that was validated, that needs investigating. Thank you, yes, I was going to ask about that.

CS-MARS

So it gives you network intelligence. So one of the nice things is it can give you topology information, where am I seeing this, traffic flow. So again, like Arbor, like Netflow, because it's taking in Netflow it can give me what kind of traffic am I seeing, device configuration and enforcement devices, so I know where my firewalls are. It gives you context correlation, context correlation is, oh that was a Windows attack against a Linux system. Well, I don't care about that, so that's a context I don't need to see because it doesn't matter. Even though it might be a valid attack in the attack sense, it's not valid against that host.

AT CISCO: IDS

So at Cisco we do use Cisco IDS. One of the really nice things about the IDS team and the InfoSec team is they work very closely together. So there are two different teams, one that does IDS, that goes through all the IDS alerts and, sorry, I sort of assumed they were part of information security. So the IDS team that's part of information security, that's true. I'm talking about the development team that makes the IDS product. Oh, I'm sorry. So we actually work closely with them in InfoSec. So InfoSec will provide feedback to the IDS development team saying, we found this, here's something new, let me test out your new product, we have a very large network and we can see how well it's going to work. So you're saying these IDS boxes have been battle-tested and battle-hardened inside Cisco, itself. Absolutely, so we're absolutely doing that. That makes sense. So we do have deployments of IDS, of course, we have them on our edges. We have them in multiple places where we consider sensitive networks, we have them deployed. Things like our extranet parameter would have them as well because we're going to be concerned about what kind of traffic's coming in from our partners because we need to protect ourselves, and so we're doing our due diligence. We do have our virtual team, that's part of information security to review and react to any alarms that do

show up. The bulk of security cases are initiated from the alarms that are found, so in talking with the incident response team within Cisco, the bulk of their cases are from the alarms. And these are alarms coming from the CSMARS system that you talked about? The CSMARS system or the event correlation, the other one that we're using is SIMs.

AT CISCO: EVENT CORRELATION

Thank you. Now I didn't talk about SIMs simply because we'd had this product for awhile and most people are aware of it. CSMARS is the newer product, make sure we had that technology background. So why do we have two products? SIMs is a product that we OEM; it's made by netForensics, we have a partnership with them and we had them first before we purchased the acquisition for CSMARS. We are currently using SIMs as our deployment for looking at IDS events. So CSMARS will do additional things that will collect Netflow, it's going to collect IDS, it'll collect syslog, it's going to integrate with CSA, it will also do some virus scan data. So we're going to be pulling all of this information into our CSMARS deployment. Sorry, integrate with CSA? How does it integrate with CSA? So CSA, we're going to talk about CSA. CSA has a management system that collects any alarms that CSA gets. Oh, of course, it logs, yes, it logs the alarms. Absolutely, so it will integrate that, so there's another piece of information to be able to look at to correlate. So CSMARS will pull all of this information; this is what we're planning on collecting initially with our initial deployments, we'll leverage them for reporting and categorization of events. So for quite some time we'll be running both SIMs and CSMARS together because we find that they both provide useful information. Sounds good. Absolutely.

SECURITY STRATEGY: PROACTIVE & REACTIVE

And the next area we want to talk about is architectural design and network segmentation, both of these areas are important because you have to have a solid architectural design to be able to have good security and part of good security's going to be your network segmentation.

BEST PRACTICE: DISABLED SERVICES

Architectural design. Now I understand architectural design to be able to provide performance and to be able to provide reliability but the design itself provides security? Absolutely, so if you're going to design a network and you want to have reliability, now if I have a DoS attack, all of a sudden my reliability goes down. Security becomes an integral part of all of the things that are part of a good design. Thank you, makes sense. And that's why we go forward and we want security to be part of that design, not an afterthought, so we consider that important. So the first thing we start with is we do have best practices, and these are industry wide best practices that Cisco follows as well. Here is listed a series of things that we consider services that you should disable. Some of them are already disabled by default in IOS 12.0, some of them are not. Some of them are ones that people turn on because they don't know what they are and so we suggest that these are ones that we consider standard good best practices to just disable. Finger..., you don't need to know who's on the device. Proxy ARP, you probably don't want your routers doing a proxy ARP connection. There's ... directed broadcasts. You can go through each of these and know these are security best practices, turn them off, we don't need them running and Cisco actually does turn them off using templates, part of our process and policy.

BEST PRACTICE: ENABLED SERVICES

You want to have certain things enabled. So, on the Cisco routers you want service password encryption. Service password encryption encrypts any passwords on the device, like line passwords, user passwords, so that when somebody's just looking at the config, they can't see them in clear text. Very good. Probably very standard. We recommend and actually in Cisco we use, SSH, so to get to any device we're actually using SSH. Instead of telnetting. Instead of telnetting, because telnetting's clear. These passwords are going in the clear and you go, whoops, there went my password, somebody could just sniff it off the network. Within Cisco, there are so many people that can get the availability to get onto our network because we have lots of partners, we have contractors and we have visitors that come in that connect to our network. So we don't want people to be able to just sniff the network and grab some of these telnet passwords, so we use SSH. Again,

some additional best practices of what we recommend for turning on part of Cisco's template for what we do for configuring any device includes making sure all of these are enabled. Sounds good, thank you.

AT CISCO: GENERAL CONFIGURATION TEMPLATE

So at Cisco, our template, as I said, we have an absolute template. We do centralized logging. So we do centralize our logging in that, from a syslog perspective, we collect all of our logs to a general location. We do it in a couple of different places. We do it in our enterprise management system, we collect the logs there, we collect logs in InfoSec, we'll be collecting logs with CSMARS. So we put down what the regional syslog server is and those regional syslog servers feed a centralized system, so that way we're not sending all our syslog traffic across wide area links. Does turning on logging slow down any of the routers and switches that the logging information's coming from? It doesn't slow down logging in general. There are certain things when we do ACLs, so when we look at ACLs and we're looking at logging, some of the information on the ACLs. If we end up with a lot of traffic on a particular ACL that we have logging information turned on, that can impact the router and we've had that on occasion, so we are very aware of that and we keep an eye on that type of information. General syslog information, what happens is if the router gets busy, it drops the syslog information and just doesn't send it out. We set a logging buffer that's pretty standard. We have an ACL for our SNMP. We only allow our enterprise management systems the ability to do SNMP gets or SNMP writes. And then we also have consistent time. Most people don't think about it, but if you don't have a consistent time against all your devices, if you have a problem and you're trying to do event correlation, how do you know when it actually happened? So we do use NTP, we have consistent time, we have regional NTP servers that each of the devices connect to.

AT CISCO: TEMPLATE INFORMATION

And in addition to that, we have a host name or a prompt and system information, so we have some type of internal host name so we know what it's called. Now we have a system that we've devised of what we call all of our devices so that I could look quickly at something and go, oh, I know what that is and I know what it's used for. Just by the name itself. Just by the name itself. Now we don't try to advertise that because then other people would know, but as a security person or a network operations person, it's very useful for me to have. We create a banner. Now why is a banner important, most people say. A banner's important because it's like a no trespassing sign. It says halt, you're not authorized to be on this device, you shouldn't be there and so the banner is what you're going to have for that. So you want to make sure you have the banner. And then of course we use the enable secret. This is our MD5 hash, it's not reversible for the enable password, which gives you the highest privilege level on the router. So that's what we do, and this is part of all of the template, part of our process for putting in a new device or a new router onto the network. And part of the architecture, too. Absolutely, part of this is what the architecture does so that we know what makes sense. Why did we do regional syslog servers, the architecture made sense to do regional, rather than trying to send all the information across the WAN links, absolutely.

AT CISCO: BEST PRACTICES

What are the other best practices we do? We have a router audit tool we run on a daily basis that will check if the devices are staying to this template. We create a list that happens that says, these devices are not meeting the template, here's where they're failing and that's given to our network operations teams, who then go and remediate the top 10 devices. How could a device not meet the template if it was setup with that template? Somebody may have gone in and changed it for some reason. It's also something to go back and check to find out who changed it, which is where our AAA services come in, and be able to find out if it was accidental or if somebody was trying to hack into the device. Very good. So all of these are reasons why things may have happened. Auto configuration of some template features. Now this is nice because, let's say somebody went in and manually changed an ACL like for SNMP. Nightly, we have some auto configuration that says, the ACL should always look like this, what it does is it says, every night it rewrites that ACL to be that. So if somebody went in and was doing something temporarily and they forgot to change it, it will get overwritten. And then we have a policy that says, we will only permit SSH as the remote access mechanism to our devices. So if you're going to go and configure a router or a switch you have to use SSH to do so. And that's a policy we have, the way we actually implement it is our networking teams actually support us in doing that.

UNICAST RPF OVERVIEW

Another feature that we want to talk about is called unicast RPF. Now unicast RPF is actually a very nice feature because one of the things that become a big concern, especially in DoS attacks is address spoofing. So that is somebody trying to take one of your addresses internally and coming from the Internet using that address. Looking like a trusted mechanism but not being so. Absolutely, absolutely. So normally how you would usually deal with that is you have to create an ACL. Now the hard thing about that is what happens when your addresses change, or what happens when something changes with your addresses, you have to go and update all those ACLs. Well unicast RPF, what it does is it helps you with that because what it can do is it will actually check on those addresses.

URPF-STRICT MODE

So strict mode, which is one of the modes that unicast RPF runs in, says, I'm going to see if the source address of the packet that's coming in, if I did a lookup on what the route should be for that, is it on the same interface that that source is coming in on? If it were really who it says it was, would it be coming in that direction. I see. Absolutely, if it's something that comes in and it says, oh, wait a minute, you should actually be coming on this other interface, it will automatically drop the packet. But there are multiple interfaces the traffic could be coming through, aren't there? Yes, there is, and that's where you get into the other mode, which is loose mode.

URPF-LOOSE MODE

So loose mode looks at it and says, is this traffic that's in my routing table at all. Now one of the things with loose mode is you do need a full routing table because it doesn't use default. So loose mode we would use at the edges like where we peer with our ISP providers. Where they have to have a full table anyway. Where we have a full table that says, am I seeing this traffic. Very useful if you're doing BGP black holing because anything that's considered a null 0 route is then dropped. So if I put a null 0 route in, it's just going to drop that traffic when it looks it up in the routing table. So if we're detecting spoofed traffic at the outer edge of our Internet connectivity then basically all that's going to get dropped before it even comes onto the Cisco network. Absolutely, and that's the whole point of it because we don't want to do that. The other thing is that we can use some of this internally, especially with the strict mode, for like on our labs to make sure they're not using addresses that are not addresses they've been assigned. So where they're not multi-homed or it's a single homed connection, we can absolutely do strict mode as well. So it stops traffic that's perhaps not malicious but traffic that's just going to mess up your routing anyway. It might mess up the routing, it might hit the firewall and cause an internal DoS problem there. So and it's usually not malicious, it's somebody's just misconfigured something and so it's just another way to protect ourselves.

AT CISCO: IOS SECURITY FEATURES

Good to drop it, yes. So what do we use at Cisco? We do use uRPF at Cisco. At the edges, we do it at our ISP edge, our building edge, our DMZ edge, our lab edge, so we've got multiple places; the edges are the most logical place to go ahead and do uRPF. We also do traffic policing or CAR, which is committed access rate, so we limit certain types of traffic at our ISP edge. Have you ever heard of a DoS attack with ICMP? Well, yes, actually quite a bit. Yes, so we can limit the amount of ICMP traffic we're going to allow in or out of our network using traffic policing. Because CAR, I always think of CAR as being a quality of service tool and here it, in fact, it is a sort of quality of service tool but for security, interesting. Absolutely, so a lot of the tools that you would normally use in your network can also be leveraged from a security perspective. So that's what we're showing here is how these same tools, that I'm going to use for other things, are also leveraged for security. Very nice. IOS firewall, also called CBAC, people use the two terms interchangeably, we're actually using that on some of our remote access devices. So with the 831, we're using IOS firewall there. So the 831 is the router, actually we have almost 7,000 routers now out in people's houses supporting home access into the network. Yes, and we're using IOS firewall on some of those. Very nice. We've approved the standard to be able to use IOS firewall for extranet. We've not deployed anything yet, but we have a standard that has gone through architectural design to allow us to be able to do it. And one of the things looked at was, how is the reliability on that, what is going to be the impact on the device itself, are we going to have throughput? So all of these questions were answered before we created the standard but now we have a security standard that's already gone through architectural design.

AT CISCO: SWITCH SECURITY FEATURES

So what are we doing on the switches? We're using several different features that exist on switches today, a lot of the switches have a variety of features that you can use to enhance your security. One of those is DHCP snooping, we're investigating usage of that on our voice VLAN because with voice, it's very important that they get their IP address. What happens when somebody accidentally brings up a DHCP server and starts giving out addresses? Right, all of a sudden I can't use my phone, I can't even call my helpdesk to say, I have a problem. So how can somebody accidentally setup a DHCP server? So there are Microsoft Windows servers that, when you load just everything by default, it automatically loads the DHCP server. And there are many people, as I said, Cisco has a culture of openness and the ability, we want people to be innovative, so sometimes they take that innovation to the point of deciding their cube is a lab. I've seen that happen, yes. And that's what happens. So we're trying to find ways of protecting ourselves and we're investigating how we can use DHCP snooping on our voice VLAN. The other one that we are using is we're using port security. We're deploying that on some of our networks. We don't deploy it across the board, we have some of our more secure networks where we believe we need it. What port security does is it says, this MAC address, or set of MAC addresses, or limited number of MAC addresses, can connect to a port. So if I've got a set of servers that are important that I want to use, and I don't want somebody coming along and. Unplugging and plugging in, yes. Yes, I would use port security. Makes sense. The other place you might use it is on you desktops. You might limit the number of machines somebody can plug into because one of the things you're protecting against is you're protecting from somebody filling up the CAM table in your switch and then causing traffic to be just broadcast. Too many desktop labs in one place, yes. Or sometimes there's people actually being malicious, trying to fill up the CAM tables to see that traffic, so when I say, telnet, I get your password, so port security helps protect us against that as well. ARP inspection. ARP inspection is something we're including in our standard for secure data center. We're only putting it there because of the overhead it requires to actually configure it and maintain ARP inspection and we've decided that, for the secure data center because we want security built in, we're going to use ARP inspection there. I have no idea what ARP inspection means, what does that really mean? ARP inspection means, have you ever had the opportunity where you could change the MAC address on your PC? I can do it, yes. Have you ever had anybody change it where they decided they were the default router? No, so far I haven't. People actually have done that where they change it and now that the MAC address of the default router, and the traffic will go to them. Got you. So what ARP inspection does is it says, this MAC address and this IP address are always tied together. Interesting, thanks. So that's where that would come in. Thank you.

HIGHLY SCALABLE MULTI-CONTEXT SECURITY SERVICES

One of the other things that we're investigating, which is another technology, is the highly scalable multi-context security services. Now that's a real mouthful, but what it really means is that I can have a single firewall services module, or single PIX, that has multiple different firewalls inside of them. Rather than having five different firewalls, I can have one, but it acts like five different ones built in. Why would I want five different firewalls in the first place? Well, so let's think about this. In our secure data center we have a set of financial applications that we want to have secured and we want them completely secured against maybe our PKI implementation, and we want a completely separate firewall context for each of those. So different policies, but all in the same firewall, all in the same engine, interesting. All in the same firewall, yes, so that is something that Cisco's actually looking at.

TRANSPARENT (LAYER 2) FIREWALL

The other thing is the L2 firewall, or transparent firewall, another feature that Cisco has internally has been very interested in. Because of what we went??? from our routing protocol perspective, we didn't want to have to move to doing static routes when we migrated to doing a stateful firewall. And what the transparent firewall does is it allows things like routing protocols to be transparent through the firewall but we still get our L3 protection at the same time. So it's a very useful feature for us to have, it's an ideal environment for areas ... IT budgets, that have limited IT budgets that need to be able to put a firewall in. It basically, if you do a trace route, you don't even see it, it's totally clear. Now the transparent firewall, what is that physically? Both the PIX and the firewall services module will both support a transparent

firewall, the PIX has a version 7.0 code, so there's a lot of information that you can do with that. There's also investigation into the IOS firewall being able to support this at some point in the future, so we absolutely have some good technology here for doing this.

AT CISCO: FIREWALLS

So at Cisco, the firewalls themselves, we use both PIXs and firewall services modules, we use them as our corporate firewall so that those eight primary locations we're using some combination of the two. We're using transparent features in those locations because we don't want to create multiple static routes. Cisco's a very large company and we have a lot of routing tables. We're using the firewall service module and the PIX also in critical networks, so not only on our primary locations but also internally within the company on places that we consider critical. Again, something like our PKI infrastructure, financials, these would be all places we may use the PIX or the firewall services module. An additional layer of protection. Yes, makes sense. Absolutely, we're planning usage of the firewall services module, even more in more parts of our data center. Part of the secure data center initiative has it as a critical point and part of that will be using the context-based firewalls that we talked about two slides ago. Thank you, yes. I was losing you there. And then we're investigating the virtual firewalls also, so we're doing a combination of things; we've got them in multiple places already, so the networking team is feeling more comfortable with using them. And it makes sense, since we have 6500s pretty much running our network within the campus, it's very easy to put an FWSM, yes. Absolutely, and so that's where that comes in play.

SECURITY @ CISCO – END OF PART 1

So we're at the end of our first section. Excellent, so we'll take a break here and we'll continue in just a few minutes with part two of security at Cisco. So what you'll need to do is you'll need to click on the second URL, which is located just below the first one that you clicked to get here, to see the exciting conclusion of our review of security technology. And in addition, we'll have a question and answer session with Laura, and as well as that, we'll have some additional resources for you to get further information on the web. So thank you for coming and we hope to see you back in part two of security at Cisco.

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 C78-337381-00 02/06