Configuring a Site-to-Site VPN Tunnel Between RV Series Routers and ASA 5500 Series Adaptive Security Appliances

Objective

Security is essential to protect the intellectual property of a business while also ensuring business continuity and providing the ability to extend the corporate workplace to employees who need anytime, anywhere access to company resources.

VPN security solutions are becoming more important for small and medium business companies. A VPN is private network constructed within a public network infrastructure, such as the global Internet. A VPN extends a private network between geographically separate office locations. It enables a host computer to send and receive data across public networks as they were an integral part of the private network with all the functionality. VPNs increase security for a distributed organization, making it easier for staff to work from different sites without compromising the network. The motivations to use VPN are the requirements to "virtualize" some portion of an organization's communications and the economics of communications.

There are different VPN topologies: Hub and spoke, Point-to-point, and Full mesh. This smart tip covers site-to-site (point-to-point) VPN, which provides an Internet-based infrastructure to extend network resources to remote offices, home offices, and business partner sites. All traffic between sites is encrypted using the IP Security (IPsec) protocol, and network features such as routing, quality of service (QoS), and multicast support are integrated.

The Cisco RV series routers deliver robust and easily managed VPN solutions to cost-conscious small business companies. The Cisco ASA 5500 Series Adaptive Security Appliances help organizations to balance security with productivity. It combines the industry's most deployed stateful inspection firewall with comprehensive next-generation network security services, including: visibility and granular control of applications and micro-applications, web security, intrusion prevention systems (IPS), highly secure remote access, and others.

This short guide describes an example of the design for building a Site-to-Site IPsec VPN between RV series routers and an ASA 5500 Series Adaptive Security appliances and provides configuration examples.
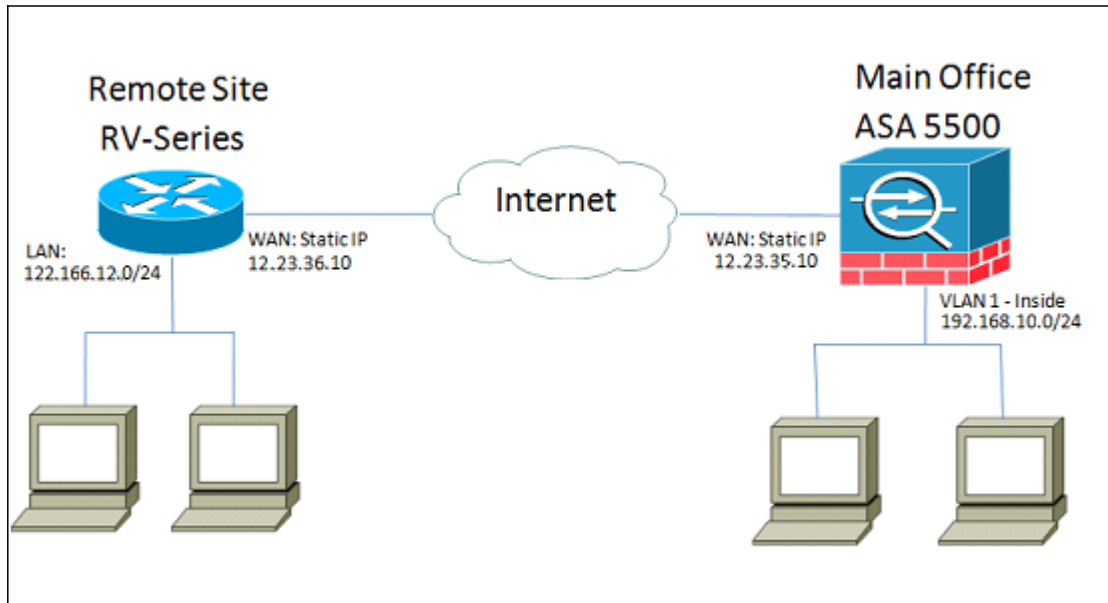
Applicable Devices

- Cisco RV0xx Series VPN Routers
- Cisco ASA 5500 Series Adaptive Security Appliances

Software Version

- 4.2.2.08 [Cisco RV0xx Series VPN Routers]

Pre-Configuration

The following image shows a sample implementation of a Site-to-Site VPN tunnel using a RV-Series router (Remote Site) and an ASA 5500 (Main Office).

With this configuration a host in the remote site network of 122.166.12.x and a host in VLAN 1at the main office can communicate with each other securely.

Key Features

Internet Key Exchange (IKE)

Internet Key Exchange (IKE) is the protocol used to set up a security association (SA) in the IPsec protocol suite. IKE builds on the Oakley protocol and Internet Security Association and Key Management Protocol (ISAKMP), and uses a Diffie-Hellman key exchange to set up a shared session secret, from which cryptographic keys are derived. A secure policy for every peer must be manually maintained.

Internet Protocol Security (IPSec)

IPsec uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. IPSec involves many component technologies and encryption methods. Yet IPSec's operation can be broken down into five main steps:
Step 1. "Interesting traffic" initiates the IPSec process - Traffic is deemed interesting when the IPSec security policy configured in the IPSec peers starts the IKE process.
Step 2. IKE phase 1 - IKE authenticates IPSec peers and negotiates IKE SAs during this phase, setting up a secure channel for negotiating IPSec SAs in phase 2.
Step 3. IKE phase 2 - IKE negotiates IPSec SA parameters and sets up matching IPSec SAs in the peers.
Step 4. Data transfer - Data is transferred between IPSec peers based on the IPSec parameters and keys stored in the SA database.
Step 5. IPSec tunnel termination - IPSec SAs terminate through deletion or by timing out.

ISAKMP

Internet Security Association and Key Management Protocol (ISAKMP) are used to negotiate the tunnel between the two endpoints. It defines the procedures for authentication, communication, and key generation, and is used by the IKE protocol to exchange encryption keys and establish the secure connection.

Design Tips

VPN topology — With a site-to-site VPN, a secured IPsec tunnel is configured between every site and every other site. A multi-site topology is usually implemented as a full mesh of site-to-site VPN tunnels (that is, every site has established tunnels to every other site). If no communication is needed between remote offices, a hub-spoke VPN topology is used to reduce the number of VPN tunnels (that is, each site establishes a VPN tunnel only to the main office).

WAN IP addressing and DDNS — The VPN tunnel needs to be established between two public IP addresses. If the WAN routers receive static IP addresses from the Internet Service Provider (ISP), the VPN tunnel can be implemented directly using static public IP addresses. However, most small businesses use cost-effective broadband Internet services such as DSL or cable modem, and receive dynamic IP addresses from their ISPs. In such cases, DDNS can be used to map the dynamic IP address to a fully qualified domain name (FQDN).

LAN IP addressing — The private LAN IP network address of each site should have no overlaps. The default LAN IP network address at each remote site should always be changed.

VPN authentication — The IKE protocol is used to authenticate VPN peers when establishing a VPN tunnel. Various IKE authentication methods exist, and pre-shared key is the most convenient method. Cisco recommends applying a strong pre-shared key.

VPN encryption — To ensure confidentiality of data transported over the VPN,encryption algorithms are used to encrypt the payload of IP packets. DES,3DES, and AES are three common encryption standards. AES is considered the most secure when compared to DES and 3DES. Cisco highly recommends applying AES-128 bits or higher encryption (for example, AES-192 and AES-256). However, the stronger the encryption algorithm is, the more processing resources it requires.

Configuration Tips

Pre-configuration Checklist
Step 1. Make sure that the ASA and the RV router are both connected to the internet gateway (the ISP router or modem).
Step 2. Turn on the Cisco RV router and then connect internal PCs, servers, and other IP devices to the LAN switch or the switch ports on the RV router.
Step 3. Do the same for the network behind the ASA. Step 4. Make sure the LAN IP network addresses are configured at each site and are indifferent subnets. In this example, the main office LAN is using 192.168.10.0/24,and the remote site LAN is using 122.166.12.0/24.
Step 4. Make sure local PCs and servers are able to communicate with each other and with the router.

Identifying WAN Connection

You will need to know if your ISP hands out a dynamic IP address or if you've received a static IP. Usually the ISP will give a dynamic IP, but you will need to confirm this to complete the configuration.

Configuring the RV042G at the Remote Office

Step 1. Log in to the Web UI and go to the **VPN > Gateway to Gateway** section. Since we are adding a LAN-to-LAN connection, the endpoints will be the gateway of each network.

Step 2. Configure the Local and Remote Endpoints on the router
a) Configure the Tunnel Name to identify it from any other tunnels you may have already configured.

b) Local Group Setup configures the local host(s) to be allowed on the VPN tunnel. Make sure that you have the correct Subnet and Mask for the network you want to be allowed over the tunnel.

Local Group Setup

Local Security Gateway Type :	IP Only ▼
IP Address :	12.23.36.10
Local Security Group Type :	Subnet ▼
IP Address :	122.166.12.0
Subnet Mask :	255.255.255.0

C) Remote Group Setup configures the remote endpoint and network traffic for the router to look for. Enter the static IP of the Remote Gateway to establish the connection in the gateway IP address field. Then enter the subnet allowed on the VPN from the remote site (the main office LAN).

Remote Group Setup

Remote Security Gateway Type :	IP Only ▼
IP Address ▼ :	12.23.35.10
Remote Security Group Type :	Subnet ▼
IP Address :	192.168.10.0
Subnet Mask :	255.255.255.0

Step 3. Configure the tunnel settings.
a) You will want to configure a pre-shared key for optimal results.
Phase 1 and Phase 2 are different phases of authentication, Phase 1 creates the initial tunnel and begins negotiation, and Phase 2 finalizes encryption key negotiation and protects the data transmission once the tunnel is established.
b) The DH group will correspond to the crypto isakmp policy group on the ASA, which you will see in the next section. On the ASA the default is Group 2, and newer versions of ASA code require at least DH Group 2. The tradeoff is that it's a higher bit and so takes more CPU time.
c) Phase 1 Encryption defines the encryption algorithm used. The default on the RV series is DES, but the default on the ASA will be 3DES. However, these are older standards and are not efficient in current implementation. AES encryption is faster and more secure, and Cisco recommends at least AES-128 (or simply AES) for best results.
d) Phase 1 Authentication verifies packet integrity. The options are SHA-1 and MD5, and either should work as they produce similar results.
Phase 2 configuration follows the same rules as Phase 1. When configuring the IPSec settings, keep in mind that the settings on the ASA will have to MATCH those on the RV042G. If there are any discrepancies, the devices won't be able to negotiate the encryption key and the connection will fail.

Note: Make sure to save the settings before navigating away from this page!

IPSec Setup

Keying Mode :	IKE with Preshared key
Phase 1 DH Group :	Group 2 - 1024 bit
Phase 1 Encryption :	AES-128
Phase 1 Authentication :	SHA1
Phase 1 SA Life Time :	28800 seconds
Perfect Forward Secrecy :	☐
Phase 2 DH Group :	Group 2 - 1024 bit
Phase 2 Encryption :	AES-128
Phase 2 Authentication :	SHA1
Phase 2 SA Life Time :	28800 seconds
Preshared Key :	c12c0VPn3x4mPL3

Configuring the ASA 5500 at the Main Office (CLI)

Note: Make sure you use the "write mem" command often to avoid losing configurations. First, here are the interfaces we have configured on the ASA. Yours may differ, so make sure to alter the configurations accordingly.

```
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.10.1 255.255.255.0
!
interface Vlan10
 nameif outside
 security-level 0
 ip address 12.23.35.10 255.255.255.0
```

Step 1. Configuring Encryption Management (ISAKMP)
The first step will be setting up the ISAKMP policy, which is what is used to negotiate the encryption of the tunnel. This configuration should be IDENTICAL on both endpoints. This is where you will configure the encryption settings to match Phase 1 from the RV configuration.

```
ASA5505(config)# crypto isakmp policy 1
ASA5505(config-isakmp-policy)# authentication pre-share
ASA5505(config-isakmp-policy)# encryption aes
ASA5505(config-isakmp-policy)# hash sha
ASA5505(config-isakmp-policy)# group 2
ASA5505(config-isakmp-policy)# lifetime 28800
ASA5505(config-isakmp-policy)# exit
ASA5505(config)#
```

Step 2. Traffic Selection
This is the same as the Local and Remote Security Group on the RV042G. On the ASA we

use access-list(s) to define what the network deems "interesting traffic" to allow on the VPN. First, configure the network objects for the remote site and local site:

```
object network insidenet
 subnet 192.168.10.0 255.255.255.0
object network rsite
 subnet 122.166.12.0 255.255.255.0
```

Then configure the access-list to use these objects:

```
access-list vpn extended permit ip object insidenet object rsite
```

Alternatively, you can use the subnets themselves, but in larger implementations it is easier to use objects and object-groups.

Step 3. IPSec Tunnel configuration (Phase 2 authentication)

Here we will configure the "Transform Set" and the tunnel group, which will set up the Phase-2 authentication. If you set up Phase-2 to be different than Phase-1, you will have a different transform-set. Here esp-aes defines the encryption and esp-sha-hmac defines the hash. The tunnel-group command configures the connection-specific tunnel information, like the pre-shared key. Use the public IP of the remote peer as the tunnel-group name.

```
ASA5505(config)# crypto ipsec transform-set asarv esp-aes esp-sha-hmac
ASA5505(config)# tunnel-group 12.23.36.10 type ipsec-l2l
ASA5505(config)# tunnel-group 12.23.36.10 ipsec-attributes
ASA5505(config-tunnel-ipsec)# pre-shared-key c12c0VPn3x4mPL3
ASA5505(config-tunnel-ipsec)# exit
ASA5505(config)#
```

Step 4. Crypto Map configuration

Now we need to apply the Phase-1 and Phase-2 configuration to a "crypto map" that will allow the ASA to establish the VPN and send the correct traffic. Think of this as tying together the pieces of the VPN.

```
ASA5505(config)# crypto map asarv 1 match address vpn
ASA5505(config)# crypto map asarv 1 set peer 12.23.36.10
ASA5505(config)# crypto map asarv 1 set transform-set asarv
ASA5505(config)# crypto map asarv interface outside
ASA5505(config)#
```

Step 5. Verify the VPN status

Finally, check the endpoints to verify that the VPN connection is up and working. The connection will not come up on its own, you will need to pass traffic so the ASA can detect it and attempt to establish the connection. On the ASA use the command "show crypto isakmpsa" to display the status.

```
ASA5505(config)# show crypto isakmp sa

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 12.23.36.10
    Type    : L2L            Role    : responder
    Rekey   : no             State   : MM_ACTIVE
ASA5505(config)#
```
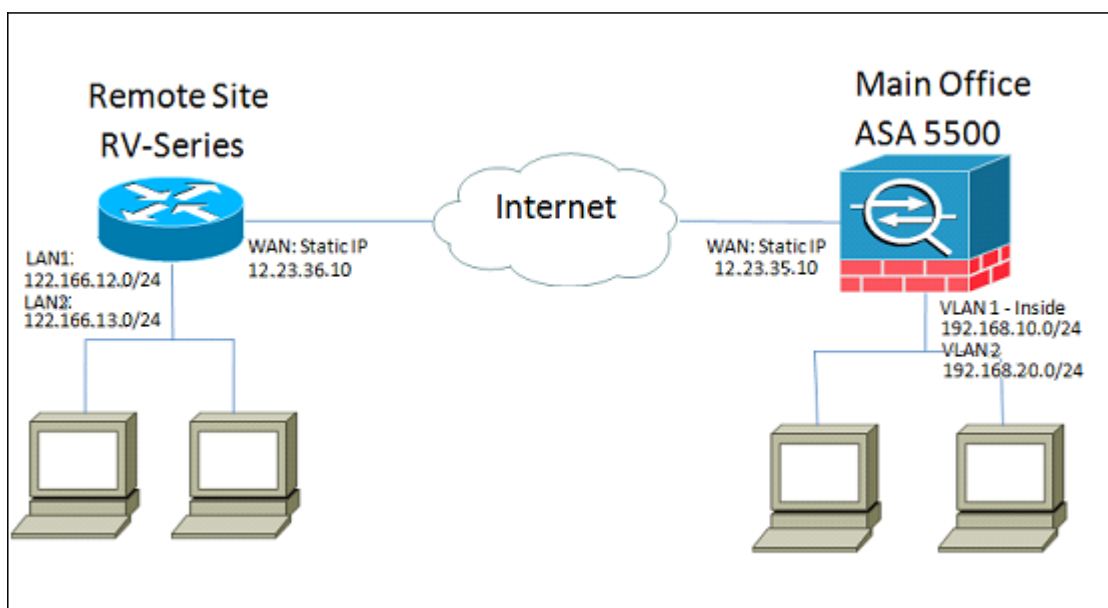
On the RV42G go to the **VPN > Summary** page and check the Status.

No.	Name	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Tunnel Test	Config.
1	TestVPN	Connected	AES/SHA1	122.166.12.0 255.255.255.0	192.168.10.0 255.255.255.0	12.23.35.10	Disconnect	📝 🗑
Add							Page 1 of 1	

Alternate Scenario: Multiple Subnets on the network

Don't panic. This can seem like an overwhelmingly complicated process when you are setting up the network, but you've already done the hard part above. Configuring the VPN for multiple subnets requires some additional configuration, but very little additional complexity (unless your subnet scheme is extensive). The example that we've used for this section uses 2 subnets at each site. The updated network topology is very similar:

Configuring the RV042G

Just like before, we will configure the RV042G first. The RV042G cannot configure multiple subnets over a single tunnel, so we will need to add an additional entry for the new subnet. This section will only cover the VPN configuration for multiple subnets, not any additional setup configuration for them.
Step 1. Configure the First Tunnel
We will use the same configuration for each tunnel as for the single-subnet example. As before, you configure this by going to **VPN > Gateway to Gateway** and adding a new tunnel, or if you are using an existing tunnel go to the **VPN > Summary** page and edit the existing

one.

a) Configure the tunnel name, but change since we will have more than one change the name to be more descriptive.

Gateway To Gateway

Add a New Tunnel

Tunnel No.	1
Tunnel Name :	VPNSubnet1
Interface :	WAN1 ▼
Enable :	☑

b) Next we will configure the local group, same as before. Configure this for only ONE of the subnets that need access. We will have a tunnel entry for 122.166.12.x and another one for the 122.166.13.x subnet.

Local Group Setup

Local Security Gateway Type :	IP Only ▼
IP Address :	12.23.36.10
Local Security Group Type :	Subnet ▼
IP Address :	122.166.12.0
Subnet Mask :	255.255.255.0

c) Now configure the remote site, again using the same procedure as above.

Remote Group Setup

Remote Security Gateway Type :	IP Only ▼
IP Address ▼ :	12.23.35.10
Remote Security Group Type :	Subnet ▼
IP Address :	192.168.10.0
Subnet Mask :	255.255.255.0

d) Finally, configure the encryption settings. Remember these settings as you will want them to be the same on both of the tunnels we are configuring.

IPSec Setup

Keying Mode :	IKE with Preshared key ▾
Phase 1 DH Group :	Group 2 - 1024 bit ▾
Phase 1 Encryption :	AES-128 ▾
Phase 1 Authentication :	SHA1 ▾
Phase 1 SA Life Time :	28800 seconds
Perfect Forward Secrecy :	☐
Phase 2 DH Group :	Group 2 - 1024 bit ▾
Phase 2 Encryption :	AES-128 ▾
Phase 2 Authentication :	SHA1 ▾
Phase 2 SA Life Time :	28800 seconds
Preshared Key :	c12c0VPn3x4mPL3

Step 2. Configuring the Second Tunnel
Now that Subnet 1 is configured for the VPN tunnel, we need to go to **VPN > Gateway to Gateway** and add a second tunnel. This second entry will be configured much the same as the first one, but with the secondary subnets from each site.
a) Make sure to name it something distinguishing so you know which connection it is.

Gateway To Gateway

Add a New Tunnel

Tunnel No.	2
Tunnel Name :	VPNsubnet2
Interface :	WAN1 ▾
Enable :	☑

b) Use the second subnet as the "Local Security" group.

Local Group Setup

Local Security Gateway Type :	IP Only ▾
IP Address :	12.23.36.10
Local Security Group Type :	Subnet ▾
IP Address :	122.166.13.0
Subnet Mask :	255.255.255.0

C) And use the second remote subnet as the "Remote Security" group.

Remote Group Setup

Remote Security Gateway Type :	IP Only ▼
IP Address ▼ :	12.23.35.10
Remote Security Group Type :	Subnet ▼
IP Address :	192.168.20.0
Subnet Mask :	255.255.255.0

d) Configure the encryption for Phase 1 and 2 the same as for the first tunnel.

IPSec Setup

Keying Mode :	IKE with Preshared key ▼
Phase 1 DH Group :	Group 2 - 1024 bit ▼
Phase 1 Encryption :	AES-128 ▼
Phase 1 Authentication :	SHA1 ▼
Phase 1 SA Life Time :	28800 seconds
Perfect Forward Secrecy :	☐
Phase 2 DH Group :	Group 2 - 1024 bit ▼
Phase 2 Encryption :	AES-128 ▼
Phase 2 Authentication :	SHA1 ▼
Phase 2 SA Life Time :	3600 seconds
Preshared Key :	c12c0VPn3x4mPL3

Configuring the ASA

Now we will modify the configuration on the ASA. This configuration is incredibly simple. You can use the same configuration as above, as it uses all the same encryption settings, with only a minor change. We need to tag additional traffic as "interesting" for the firewall to send it over the VPN.   Since we use an access-list in order to identify interesting traffic, all we need to do is modify this access-list.

Step 1. To start with, delete the old access-list, so we can modify the objects in the ASA. Use the "no" form of the command to remove configurations in the CLI.

Step 2. Once the ACL is removed, we want create new objects for the new subnets involved (assuming you haven't already done this in setting those subnets up). We also want to make them more descriptive.

Based on our VLAN configuration below:

```
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.10.1 255.255.255.0
!
interface Vlan2
 nameif engineering
 security-level 100
 ip address 192.168.20.1 255.255.255.0
!
interface Vlan10
 nameif outside
 security-level 0
 ip address 12.23.35.10 255.255.255.0
```

We need an object group for the main internal network (192.168.10.x) and the engineering network (192.168.20.x). Configure the network objects like so:

```
ASA5505(config)# show run object
object network ASAvlan1
 subnet 192.168.10.0 255.255.255.0
object network ASAvlan2
 subnet 192.168.20.0 255.255.255.0
object network RVvlan1
 subnet 122.166.12.0 255.255.255.0
object network RVvlan2
 subnet 122.166.13.0 255.255.255.0
```

Step 3. Now that the relevant network objects have been configured, we can configure the access-list to tag the appropriate traffic. You want to make sure you have an access-list entry for both networks behind the ASA to both remote subnets. The final result should look like this.

```
ASA5505(config)# show run access-list
access-list vpn extended permit ip object ASAvlan1 object RVvlan1
access-list vpn extended permit ip object ASAvlan1 object RVvlan2
access-list vpn extended permit ip object ASAvlan2 object RVvlan1
access-list vpn extended permit ip object ASAvlan2 object RVvlan2
```

Step 4. Now, because we deleted the old access-list, we need to reapply it to the crypto map using the same command as before:

```
ASA5505(config)# crypto map asarv 1 match address vpn
```

Verify the connection

And that's it! Your tunnel should be operational now. Initiate the connection and check the status using the "show crypto isakmpsa" command on the ASA.

```
ASA5505(config)# show crypto isakmp sa

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 12.23.36.10
    Type    : L2L               Role    : responder
    Rekey   : no                State   : MM_ACTIVE
ASA5505(config)#
```

On the RV-series the status will be displayed in the VPN > Summary page.

No.	Name	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Tunnel Test	Config.
1	VPNSubnet1	Connected	AES/SHA1	122.166.12.0 255.255.255.0	192.168.10.0 255.255.255.0	12.23.35.10	Disconnect	
2	VPNsubnet2	Connected	AES/SHA1	122.166.13.0 255.255.255.0	192.168.20.0 255.255.255.0	12.23.35.10	Disconnect	
Add							Page 1 of 1	

View a video related to this article...

Click here to view other Tech Talks from Cisco